Government of Canada | Gouvernement du Canada

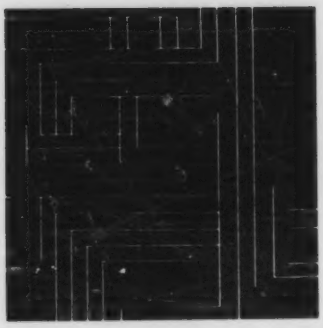
THE PROTECTION OF PERSONAL INFORMATION

BUILDING CANADA'S INFORMATION ECONOMY AND SOCIETY

Summary Report
of the Responses to the
Discussion Paper

July 1998

Canada



THE PROTECTION OF PERSONAL INFORMATION

BUILDING CANADA'S INFORMATION ECONOMY AND SOCIETY

Summary Report
of the Responses to the
Discussion Paper

July 1998

This publication is also available electronically on the World Wide Web at the following address:
http://strategis.ic.gc.ca/privacy

This publication is also available in alternative formats on request.
See distribution contact numbers listed below.

For additional copies of this publication, please contact:

Diane Breau
Electronic Commerce Task Force
Industry Canada
300 Slater Street, Room 2052C
Ottawa, ON K1A 0C8

Tel.: (613) 991-4029
Fax.: (613) 941-0178
Email: breau.diane@ic.gc.ca

Murray Long may be contacted at:

Murray Long Communications and Policy Consulting
640 LaVerendrye Dr.,
Gloucester, ON K1J 7C4

Tel.: (613) 747-9651
Fax.: (613) 747-6261
Email: murray.long@sympatico.ca

©Her Majesty the Queen in Right of Canada (Industry Canada) 1998
Cat. No. C2-355/1998
ISBN 0-662-63706-2
52007B

Aussi disponible en français sous le titre *La protection des renseignements personnels : Pour une économie et une société de l'information au Canada – Rapport sommaire des réponses au document de travail.*

Contents

Introduction	1
Executive Summary	5
Detailed Analysis of Submissions	11
Obligations	11
Powers	39
Distribution of Powers and Responsibilities	52
Cooperation	65
General Conclusions	70
Appendix 1. Index List of Submissions	71

102-05206/

Introduction

On January 27, 1998, Industry Canada and the Department of Justice released a consultation paper entitled *The Protection of Personal Information - Building Canada's Information Economy and Society*. A total of 83 submissions were received by the March 27, 1998 deadline for response, ranging from detailed submissions from industry associations to single page e-mails from private citizens. An additional seven submissions were received after the deadline. All seven late submissions are included in this analysis.

Of the 90 submissions, 22 were from individuals; included in this category were three from academics, four from privacy experts or consultants, and one from a member of the Alberta Legislature.

Among organizations, the federal Privacy Commissioner and the privacy commissioners for Alberta, British Columbia, Ontario and Quebec all responded. There were 10 submissions from consumer groups, one submission from a labour organization (the Canadian Union of Public Employees), four submissions from organizations within the health care sector, five submissions from organizations representing archivists, historians, librarians and records managers, and one submission from a law enforcement agency (the Royal Canadian Mounted Police). The Government of Alberta submitted a response, as did the European Union.

Among responses from business groups, there were five submissions from industry associations whose membership have an interest in information technology and electronic commerce issues. These were the Advanced Card Technology Association of Canada (ACT), the Canadian Association of Internet Providers (CAIP), the Canadian Advanced Technology Association (CATA), the Canadian Information Processing Society (CIPS), and the Information Technology Association of Canada (ITAC). There were seven submissions from business organizations representing both conventional retail and direct marketing interests. There was one submission from an organization representing media interests, the Canadian Newspaper Association. There were six submissions representing the positions of telecommunications companies subject to federal regulation through the Canadian Radio-television and Telecommunications Commission (CRTC), and three from the cable television industry, which is also subject to CRTC regulation. There were two submissions from organizations representing federally regulated financial institutions, and 14 additional submissions representing both federally and provincially regulated companies within the financial, insurance, securities, and credit reporting industries, as well as professional associations within this broadly defined sector.

In our analysis of submissions, we had to reflect on many thoughtful and original suggestions on how to construct, implement and enforce privacy legislation. On some points, there is a consensus of opinion. As might also be expected, some suggestions are diametrically contradicting. While these may represent both ends of the spectrum on a certain issue, in most cases, other suggestions present a degree of flexibility on how some issues might be addressed.

On some issues, there is as much divergence of opinion between sectors and within sectors as there is convergence. This applies equally to privacy commissioners, consumer groups, individuals and business organizations.

Moreover, within the business community, some submissions reflect the views of groups of professionals that work within an industry sector and, as such, the approach to issues is considerably different than the viewpoints of business organizations themselves. Business organizations may be subject to differing oversight regimes — federal, provincial, or both — or have no regulatory oversight.

Finally, there were a wide variety of models suggested as to how privacy protection could best be achieved within the commercial marketplace. As a result, it was a challenge to organize and compare the various responses in any meaningful way. The reader, however, benefits from knowing where particular views come from, and to what extent there are common opinions and views, or views that reflect a "business position," a "consumer position," or the position of privacy commissioners, for example.

To make the task of sorting out positions somewhat easier, categories of respondents have been organized as follows: Privacy Commissioners; Consumer Groups (including organized labour); the Health Care Sector; Law Enforcement; Government, including the European Union; Institutes; Archivists/Historical/Library Associations; the Telecommunications/Cable Sector; a broadly defined Financial Sector; Commercial/Retail Organizations; Information Technology Associations; and Individuals (including consultants, experts and academics). There may be some respondents to the Industry and Justice Canada discussion paper that feel this arbitrary grouping of interests does not fairly or accurately characterize their position within the overall community of interests. For this we apologize.

Some respondents provided insightful comments on their perceptions on the need for an information protection law, or detailed analysis on how their industry group currently protects personal information. We have chosen largely to omit these more general background comments in the summaries and focus instead on the specific responses to the 15 questions posed in the discussion paper. As a result, comments of some individual submissions are as long or almost as long as those of large organizations.

Readers seeking more detail and clarification of positions than exists in this analysis are urged to read the summaries. In addition, where even more specific detail is sought, readers can contact the Electronic Commerce Task Force for copies of selected submissions, many of which offer considerably more information on privacy issues and concerns, and private sector privacy initiatives than this document can possibly convey.

Murray Long

Suzanne Andrew

Executive Summary

There were 90 responses to Industry Canada and Justice Canada's discussion paper, *The Protection of Personal Information - Building Canada's Information Economy and Society*, ranging from detailed submissions from industry associations to single page e-mail notes. Among these submissions were two surveys, one done by the Metropolitan Halifax Chamber of Commerce among its 1400 corporate members, and the second conducted via the Internet by Privacy Forum Partners, a coalition of consumer groups, the Media Awareness Network and the Ottawa Public Library. The Chamber of Commerce survey elicited a range of opinion from support for simple legislation to strong opposition. Eighty percent of the 51 respondents indicated that legislation would have an impact on their business. The Privacy Forum Partners received 270 responses, all highly supportive of privacy legislation.

Submissions received from all parties responding to the Industry and Justice Canada discussion paper were summarized and analyzed in accordance with the 15 questions, although some comments were outside the scope of the discussion paper. Some submissions, both within the business community and among non-business groups, treated only a subset of the 15 questions and limited their comments to the issues of greatest interest to them.

To facilitate analysis, the submissions have been arbitrarily grouped into the following categories: Privacy Commissioners; Consumer Groups (including organized labour); the Healthcare Sector, Law Enforcement; Government including the European Union; Institutes; Archivists/Historical/Library Associations; the Telecommunications/Cable Sector; a broadly defined Financial Sector; Commercial/Retail Organizations; Information Technology Associations; and Individuals (including consultants, experts and academics).

Responses to a number of the questions indicated clear support for a particular direction. For example, the Canadian Standards Association *Model Code for the Protection of Personal Information* (CSA Standard) is almost unanimously regarded as the right place to start in drafting legislation, although privacy commissioners, consumer groups and some business organizations believe there is a need to add further obligations or make the legislation more precise than the existing CSA Standard.

There is also near-unanimous agreement on the need to harmonize federal and provincial privacy laws to ensure consistent application, prevent barriers to inter-provincial trade and discourage the growth of data havens. There is also strong agreement that the Uniform Law Conference of Canada (ULCC) represents the best overall forum to achieve harmonization of federal and provincial privacy legislation.

There is widespread support for the Office of the Privacy Commissioner of Canada to be

the oversight agency, and broad agreement that the Office of the Privacy Commissioner is the best body to educate the public about privacy matters.

Regarding sectoral codes, there is strong agreement that such codes play a useful role in protecting personal information, but there is little support for such codes replacing the law. There is also little support for start-up obligations such as registration of privacy codes with an accredited registrar or oversight body.

On several other questions there was a wide divergence of opinion. These included the question of disclosure without consent and exemptions to the legislation, as well as questions on enforcement powers, the creation of a tribunal or use of the Federal Court, the role of existing industry regulators and the requirement for privacy impact assessments.

On the issue of whether or not the CSA Standard is precise enough in setting out obligations, privacy commissioners, consumer groups, and individuals generally all believe changes are required to make the Standard more precise and add new obligations, such as a requirement to justify information collection purposes. Some business organizations also believe legislation would require more specificity to enable certain types of information-gathering and use, and to set clear and predictable rules under which businesses can operate.

Because the submissions from both consumer and business groups indicate a common concern about the need for precision, it would seem to make sense to revisit the CSA Standard in an attempt to accommodate these concerns. In their attempts to contribute to greater business certainty about information uses, some of the detailed suggestions provided in the submissions, however, may impinge on the flexibility of the current CSA Standard, an aspect of the CSA Standard that the majority of businesses assert should be maintained.

The majority business view is that the CSA Standard not be altered in any way, since it provides the flexibility necessary for business activities. Businesses noted that they require a light-handed legislative framework that does not unduly impede business activities. It may be possible to achieve the right balance by jointly examining issues of precision and obligations with the nature of the oversight powers proposed by different parties. In this case, the less precise the law is, the greater the oversight powers may need to be, and vice versa, to ensure that information privacy rights are adequately protected and an appropriate balancing of interests is maintained.

The issue of disclosure without consent and exemption to the legislation provides another opportunity to find a balance of interests that might accommodate the needs of all parties. Archivists and the media seek exemptions from the scope of the legislation for historical information and journalistic activities. Instead, including both activities as types of information that might be subject to use and disclosure without consent might accommodate these activities, while still ensuring other privacy protection principles, such as accountability, purpose definition and safeguards remain in place.

In the area of complaints investigation, there is general acceptance by all parties that consumers should deal directly with organizations first, and only when a complaint cannot be resolved should an oversight body become involved. There is clear support for the federal Privacy Commissioner having ultimate oversight responsibilities. There is very little support for federal sector regulators, such as the Canadian Radio-television and Telecommunications Commission (CRTC) or the Office of the Superintendent of Financial Institutions (OSFI), having ultimate oversight responsibilities. There is, however, some support for industry self-regulatory organizations to assist in the complaints resolution process.

In addressing enforcement powers, there is broad support, although not unanimous among business interests, for proactive oversight powers that would include investigation, independent of complaints. There is, however, a range of opinions on how compensation should be awarded. There are also mixed views on whether privacy assessments should be mandatory, and how they should be performed.

Highlights

The Highlights below draw from the Detailed Analysis section of this report where they are elaborated upon in greater detail. They represent the diversity of opinions expressed by respondents. In some cases, the authors have offered some suggestions to accommodate the interests of all parties.

(N.B. Conclusions are numbered and organized on the basis of the 15 questions within the consultation paper.)

1. It is generally agreed that the CSA Standard should be the basis for legislation. However, comments by various parties, including privacy commissioners, consumer groups, business organizations, special interest groups and individuals, on the need for greater precision and additional obligations should be considered in any drafting exercise.

2. Various business organizations and other parties suggested specific categories of information use that should be subject to disclosure without consent. Other parties, including privacy commissioners and consumer groups want an extremely limited and highly specific list of information use categories and situations where disclosure without consent would be allowed. It was also noted by some parties that no such list can be exhaustive. In light of these differing positions, the best approach may be to include a well delineated list of examples of disclosure without consent within the legislation, and guidance on circumstances under which such disclosures would normally be allowed. The suggestion made by a few parties that organizations be required to document and substantiate any such disclosures without consent is also worth consideration.

3. There is limited support for binding sectoral codes, and it is generally suggested by respondents that there be no provision within legislation to allow sectoral codes to replace legislation or have legal recognition, including interpretative value. One business submission, in particular, raised the issue of the interpretative value of such codes (i.e. courts, in determining penalties or awards would have to give due consideration to the manner in which the organization interpreted the legislation within its sectoral code). One consumer submission, however, suggested that a fundamental reason why greater precision is required within the legislation is to prevent organizations from using the "impenetrable defense" that they have applied subjective judgement to the CSA Standard in good faith. Perhaps, given these conflicting views, the question of interpretative value is best left to the courts without any direction within legislation.

4. The submissions indicate that the legislation should define "person" to include only natural persons to avoid giving organizations the information protection rights of individuals. The drafters of legislation should also consider whether to distinguish between widely available public domain information and public information that is not intended for widespread distribution or use. Where categories of data users seek exemptions from the legislation, the drafters should consider whether to exempt users from the full scope of the legislation or whether exemptions, if any, should be restricted to particular aspects (e.g. an exemption from the obligation to obtain consent before information collection, use or disclosure).

5. Support for registration procedures, where it existed, seems to be on the merits of creating a central repository of codes and contact individuals. Given the lack of support for this concept from privacy commissioners, and the availability of such information directly from organizations under the law, a registration process appears to be unnecessary.

6. Generally, all parties recognize the need for investigative powers when a complaint arises. Where detailed powers are recommended, they are generally in line with the existing powers of the federal Privacy Commissioner.

7. Consumer groups and privacy commissioners favour broad powers to address violations. Most parties support the power to publicize consumer complaints and non-compliance, without fear of liability, and several business and consumer groups as well as individuals suggest this is among the most important deterrent powers.

8. There is broad agreement that oversight bodies should have powers to conduct independent research *of a general nature*, since such research on new technologies and emerging privacy issues is of value to all parties. Most business submissions oppose proactive investigations, while privacy commissioners, consumer groups and individuals support broader powers to conduct investigations where multiple complaints, investigation and mandatory mediation suggest systematically inadequate information practices.

9. Most respondents agree that the federal Privacy Commissioner should be the oversight agency.

10. There is mixed support for the use of tribunals versus the Federal Court, and little in-depth discussion of the pros and cons of either approach. The majority of business groups prefer use of the Federal Court. Privacy commissioners and consumer groups are divided on the issue. Where a tribunal is preferred, it is generally on the basis of accessibility (e.g. the courts are clogged) and, in a few suggestions, to act as a national body that could play a role in harmonizing privacy protection across all jurisdictions (as in the Human Rights Tribunal or Competition Tribunal that were mentioned by a few parties as examples of such national bodies). Where a preference for the Federal Court exists, there is also mention in submissions from some consumer groups that the legislation should not prevent individual access to lower courts, such as provincial small claims courts, to claim damages and seek awards. In one consumer group submission, there is reference to a structured approach that would facilitate such legal actions.

11. There is clear support for the federal Privacy Commissioner having ultimate oversight responsibilities. There is very little support for federal sector regulators, such as the Canadian Radio-television and Telecommunications Commission (CRTC) or the Office of the Superintendent of Financial Institutions (OSFI), having ultimate oversight responsibilities. There is, however, some support for industry self-regulatory organizations to assist in the complaints resolution process.

12. Most respondents agree that public education should be the primary responsibility of the federal Privacy Commissioner. It should be listed as a duty under the proposed legislation, and adequate funds should be provided for it. Organizations should have an obligation to be open to the public about their own specific information use policies and practices, as specified within the CSA Standard.

13. There are differing views on the need for mandated privacy impact assessments. Business organizations are almost unanimously opposed to mandatory assessment which, in their view, might threaten technology innovation, create impossible hurdles for cash-strapped small companies and drive activities and jobs to other jurisdictions. Consumer groups have mixed views on mandatory assessments and who should perform them, and only one privacy commissioner supports legislated privacy assessments. It may be possible to accommodate the interests of all parties in protecting personal information while not unduly impacting the advance of new technologies and services by encouraging, rather than requiring, privacy impact assessments under legislation. Such assessments could be performed by accountable individuals within organizations and would be a consideration in any subsequent investigation by the federal Privacy Commissioner.

14. Most parties believe that harmonization is important, even critical, to the success of any legislated private sector privacy regime and to the marketplace, yet there are few specific instructions on how to accomplish harmonization. There are conflicting views on whether the federal government should move unilaterally on legislation ahead of the provinces.

15. There is strong support for the work of the Uniform Law Conference of Canada (ULCC), which is drafting a model privacy law, but other forums should also be used to advance harmonization of privacy protection across all jurisdictions. All forums should involve stakeholder input to the maximum extent.

Detailed Analysis of Submissions

This analysis of comments and recommendations made to Industry Canada from the various submissions follows the order of the questions from Part 3 (*Your Turn*) of the consultation paper. A range of specific detailed suggestions about implementing privacy legislation in the private sector has been captured, but should not be considered as exhaustive. For further detail, refer to the submissions.

Obligations

1. Is the CSA Standard the base from which to start in drafting legislation? Is it precise enough in setting out obligations or do some obligations require further elaboration? Are there any additional obligations not set out in the CSA Standard that should be included in the legislation?

Question 1 elicited the largest number of comments of any question. This reflects a wide divergence of opinion on private sector privacy legislation and how it should be approached.

All privacy commissioners, consumer groups, public institutes, academics, privacy experts, consultants and other individuals fully support legislation. The European Union and Alberta Government submissions also support moving forward with a federal private sector privacy law, although the Alberta Government strongly stresses the need for ongoing consultation with the provinces before any federal legislation is enacted.

In contrast, not all respondents within the private sector accept that legislation is necessary. For example, the Canadian Gas Association and Faneuil ISG Inc., a direct marketing firm, state that additional privacy protection is unwarranted at this time. Equifax Canada believes that privacy law should not proceed without empirical evidence that voluntary codes are inadequate. Credit Union Central of Canada also believes voluntary codes are preferable to law.

The majority of responses from the federally regulated telecommunications and cable industries also state a preference for privacy self-regulation. Within the federally regulated banking industry, the Canadian Banking Ombudsman is less supportive of private sector privacy law than is the Canadian Bankers Association. Among other industry submissions, the views on the need for a private sector privacy law range from clear support and acceptance to a preference for voluntary codes. Total responses reveal that, of 39 business organizations responding to the consultation paper, 17 favour legislation, 12 do not, and six organizations are ambivalent.

Regardless of their views on the need for legislation, virtually all respondents accept the CSA Standard as a good starting point. The CSA Standard is seen by almost all parties as a document that was developed by consensus, with input and broad support from industry, government, and consumer organizations.

Views differ widely, however, on whether the CSA Standard should be adopted as is, or whether it requires more precision.

Privacy commissioners, consumer groups, and most individuals favour greater precision. The federal Privacy Commissioner, in particular, offers specific and detailed wording changes to the CSA Standard. In contrast, the majority of business organizations would prefer to see the CSA Standard adopted without any changes. Their view, generally, is that the CSA Standard provides necessary flexibility for business and that more onerous requirements could stifle private sector activity.

Not all business organizations agree on this point, however. In response to *Question 1*, as well as *Questions 2 & 4*, which deal specifically with the content of the CSA Standard, a number of business organizations call for more precision where it would create "clear and predictable rules" and promote certainty in matters of interpretation, as well as meet the needs of their industry.

The comments made by those seeking greater precision cover a range of issues, although there is a strong focus among privacy commissioners, consumer groups and individuals on greater specificity in defining information collection purposes and ensuring that defined purposes are legitimate. Other key concerns are the use of implied consent, how consent should be obtained, and how data should be protected when it is processed either by third parties or outside of Canada. This question also elicited comments on several side issues that are related to personal information collection and use, such as surveillance, e-mail privacy, and the collection and use of biometric data.

The viewpoints on the use of the CSA Standard and other issues are described below by category. Please note that not all respondents answered all questions. In the responses to each question, comments appear only where specific organizations or individuals chose to make them.[1]

---

[1] There were a number of instances where the views of organizations or individuals on specific issues are ambiguous and no clearly defined position could be determined. In such cases, views are generally not represented. Also, in a small number of instances, organizations or individuals proposed a model for privacy regulation that did not correlate with some of the questions. Rather than attempt to fit the model to the question, some of these comments have been omitted here, but can be found in the individual submissions.

Privacy Commissioners

Responses were received from the Privacy Commissioner of Canada (federal Privacy Commissioner), the Information and Privacy Commissioner of Alberta, the Information and Privacy Commissioner for British Columbia, the Information and Privacy Commissioner of Ontario and the Commission d'accès à l'information du Québec (Commission d'accès).

All privacy commissioners support statutory privacy legislation, but all view the CSA Standard as requiring substantive improvements if it is to become the basis for a privacy law.

The federal Privacy Commissioner provided specific comments on each of the CSA Standard's 10 principles. This was the only submission suggesting precise wording changes to the CSA Standard. The main points appear below:

- Under *Accountability*, add a provision that organizations are legally responsible for information provided to third parties for use on their behalf.

- Under *Identifying Purposes*, add a provision that, before any personal information is collected, the purposes be both assessed and documented (and be lawful), and the individual be informed of purposes, the obligatory or voluntary nature of their consent, the consequences of failing to consent, the recipients of the information and its uses.

- Under *Consent*, add a provision that consent be plainly and clearly explained, freely given, informed, specific and express concerning all types of information uses and potential recipients, and authorized for a limited period.

- Under *Limiting Collection*, add a provision that information collection be limited to that which is required by law or for the specific identified purposes, and be collected directly from the individual, except where health or safety is directly at risk or as required by law.

- Under *Limiting Use, Disclosure, and Retention*, add a provision that personal information be used or disclosed only for the specific purposes for which it was collected and with the consent of the individual, except for health and safety or as required by law, and that such information not be disclosed without comparable safeguards, and that it be retained only as long as necessary for the purposes and securely destroyed thereafter. All personal information should be treated as confidential and released only to those who need to know, and with a confidentiality agreement for third parties. No other releases should take place without the knowledge or consent of the individual or as required by law.

- Under *Accuracy*, replace "used" with "used or disclosed."

- Under *Safeguards*, add a provision that organizations and their agents shall protect personal information by physical, organizational and technological safeguards against accidental or unauthorized access, modification or destruction.

- Under *Openness*, replace "unreasonable effort" with "unreasonable cost or effort" and add that organizations should make available specific information about their management of personal information and their complaints resolution policies and practices.

- Under *Individual Access*, replace the wording of the principle with: "Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to his or her information without cost or unreasonable effort, except as legally allowed. An individual shall be able to challenge the accuracy and completeness of the information and have it amended, updated or deleted as required by the circumstances. Access, correction, amendment and deletion requests shall be addressed within set time limits."

- Under *Challenging Compliance*, add a provision that organizations must respond to challenges within set time limits and that, if the individual remains dissatisfied with an organization's response, the individual shall have the right to appeal the response to the central oversight agency.

The Information and Privacy Commissioner of Alberta views implied consent as inconsistent with fair information practices and recommends that legislation specify consent in writing. The Commissioner adds that the law should require individuals to be advised when information is released to a third party without consent.

The Information and Privacy Commissioner for BC does not support the CSA Standard as a basis for legislation and calls upon the government to base legislation upon the far stronger information protection provisions of the *European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive) and the *B.C. Freedom of Information and Protection of Privacy Act.*

The Information and Privacy Commissioner of Ontario recommends an opening section within the legislation to better define purposes, and greater clarification of acceptable purposes for information collection in order to narrow and solidify the *Limiting Collection* principle of the CSA Standard.

The Commission d'accès suggests Québec's *Bill 68, An Act Respecting the Protection of Personal Information in the Private Sector* (the Québec *Act*) is a better basis for legislation than the CSA Standard.

Consumer Groups (including organized labour)

A total of 11 submissions were received from consumer and public advocacy groups, including the Canadian Union of Public Employees (CUPE). However, the number of actual consumer and public interest groups represented by these submissions is considerably greater.

The British Columbia Public Interest Advocacy Centre submitted comments on behalf of nine other organizations in B.C., collectively known as BCOAPO (*see the Index for a listing of these groups*). The Fédération nationale des associations de consommateurs du Québec and Option Consommateurs (FNACQ/OC) filed a joint submission, and a group known as the Privacy Partners Forum (Privacy Partners) filed a submission which included results of an electronic survey conducted jointly by seven organizations.

All consumer organizations support a federal private sector privacy law, but none believe the CSA Standard is currently sufficient as a basis for legislation.

The B.C. Civil Liberties Association (BCCLA) believes the CSA Standard should incorporate a new principle of justification to limit information collection to legitimate reasons, with organizations required to justify purposes if challenged. BCCLA notes references to "a serious and legitimate reason" in Section 4 of the Québec *Act* and to "legitimate purposes" in Article 6 of the EU Directive as a precedent for a principle of justification. BCCLA adds that privacy legislation must also apply to the process of intruding on privacy, stating that practices of organizations such as mandatory drug-testing of employees impinge on privacy interests, even if no personal data is ultimately extracted.

The B.C. Freedom of Information and Privacy Association (FIPA) supports the principle of justification and adds that a right of privacy should ultimately be incorporated into the *Canadian Charter of Rights and Freedoms*. This view is shared by Canada's Coalition for Public Information (CPI), Privacy Partners, and the Public interest Advocacy Centre (PIAC).

CPI also believes legislation should incorporate both the CSA Standard and the fair information practices contained within the Industry Canada consultation paper.

The Consumers' Association of Canada (CAC) says negative option consent should not be allowed in the legislation, with any exceptions fully justified. The purpose for data gathering should be stated precisely and data mining should be prohibited. The CAC also suggests addition of the 12 principles of the New Zealand Health Information Privacy Code.

The Consumers' Association of Canada - Ontario (CAC Ontario) supports the CSA Standard as a basis for legislation, with no comment on additional obligations. The Consumers Council of Canada (CCC) also supports the CSA Standard, but adds that individuals should have sole rights of ownership to their personal information and rights to control use.

FNACQ/OC believes new private sector privacy law could be based on the CSA Standard, but also upon the ULCC draft and the Québec *Act*, which offers more detail on obligations.

Privacy Partners opposes vague or general statements of purposes and states that legislation must precisely define consent so the individual knows permission is being sought, and

is cognizant of how data will be collected and used. All uses should be based on an opt-in provision with consent in writing wherever practical. Purposes should be highly specific with no denial of services or other penalties for refusing consent to unnecessary information collection. There must be a clear limitation period for information use and specific consent should be required to share information with other affiliated or non-affiliated organizations or departments of a company. Special protection is required for genetic and health information, and parents and guardians should control use of children's information.

Privacy Partners adds that the consultation paper definitions of privacy and informational privacy should be incorporated into the legislation. Since employees may be the only people within organizations aware of information misuses, the legislation should also contain special protection for whistle blowers.

In addition, PIAC wants a privative clause in legislation denying parties the right to contract out of legislation. PIAC also suggests that two of the *Telecommunications Privacy Principles* be added to the legislation. These principles call for privacy considerations to be addressed specifically when new services are provided and, when a new service that compromises privacy is introduced, that appropriate measures be taken to maintain customers' privacy at no extra cost unless there are compelling reasons for not doing so.

PIAC also wants the definition of "organization" to be tightened in legislation to address information use by affiliates or the rights of individual data subjects in the event of a merger. PIAC adds that, unless the law has a substantive statutory limitation on information collection purposes, the consent requirement should provide more guidance on an organization's obligations to notify the individual about information uses, especially when implied consent is used. Legislation should also set a time limit after which destruction of personal information must proceed unless the company can prove continuing need. Once a customer relationship ends, data should be depersonalized or destroyed.

BCOAPO adds that greater specificity is required to prevent organizations from using the "impenetrable defence" that they have applied subjective judgement to the CSA Standard in good faith. BCOAPO proposes written consent as the norm, suggesting that, when implied consent is used, there should be an onus on organizations to show that consent was actually given. BCOAPO adds that lack of specificity in purposes should be a basis for invalidating consent to information collection, retention or transfer. BCOAPO calls mere documentation of purposes a "meaningless exercise."

CUPE believes federal legislation should encompass companies contracting with the federal government as well as federally regulated companies, and that contracting-out of information processing or situations where private corporations gain access to sensitive data should be governed by strict rules. CUPE adds that legislation must limit use of worker personal data only for purposes for which it was collected and only for reasons directly relevant to employment. All data should be secured with reasonable safeguards, with special protections for

medical data. Workers' personal data should not be communicated to third parties without express written consent except in emergency situations, as required by law, or as necessary for the conduct of the employment relationship. Workers should be regularly notified about the personal data held about them.

CUPE also notes specific concerns about health information, stating that legislation should affirm the principles of the *Canada Health Act* governing both public and private sectors, differentiate between health information for the public good and commercial interests, protect patient privacy and confidentiality of health data, ensure that personal health information is used only for its originally intended purpose, and exclude third parties such as insurance companies, employers and pharmaceutical companies from having direct access to health information.

Health Care Sector

IMS Canada (IMS) and the Canadian Dental Association (CDA) believe the CSA Standard is the right place to start, although CDA adds that the issue of self-determination of health records should be addressed. The Canadian Institute for Health Information (CIHI) recommends the legislation differentiate between person-identifiable, non-identifiable and anonymous data. CIHI would also like to see a differentiation between private non-profit and private for-profit uses. The Canadian Nurses Association (CNA) also wants the identifiable/non-identifiable issue to be addressed, with a differentiation between commercial and public interest uses. The CNA adds that the law must allow extended retention of specific information, especially if it can be rendered anonymous, and must also provide an avenue to seek the agreement of the data subject to use data for non-intended purposes.

Law Enforcement

The Royal Canadian Mounted Police (RCMP) recommends that legislation be strengthened to include certain security principles, including the application of safeguards throughout the information lifecycle, education on principles and safeguards for data owners and users, regular evaluation of safeguards including risk assessments, a requirement that non-traditional work or information storage environments (e.g. telework and data storage services) not diminish data security responsibilities, and the application of standards consistently across information management systems.

Government (including the European Union)

The Alberta Ministry of Science, Research and Information (Alberta) supports the CSA Standard as a basis for legislation, but adds that the unique privacy requirements of personal health information may require a separate legislative framework.

The Director General of DGXV (Internal Market and Financial Services) of the European Commission (EU) also supports private sector legislation in Canada based on the CSA Standard, recommending that a provision on data transfers outside of Canada be included in the law.

Institutes

The Fraser Institute would prefer to see privacy protection within the private sector dealt with through existing law rather than incorporating a whole new system of regulation. Violation of privacy should be prosecuted as theft, subject to immediate and heavy sanction. The courts should be relied upon to incorporate theft of privacy into the existing body of law.

The University of Ottawa Human Rights Research and Education Centre (the U of O Centre) wants the law to incorporate a number of recommendations from the proposed Charter of Privacy Rights from *Privacy: Where Do We Draw the Line?*, the Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities. These recommendations state that everyone is the rightful owner of their personal information; everyone is entitled to expect and enjoy anonymity unless the need to identify individuals is reasonably justified; and exceptions infringing on privacy rights should only be allowed if the interference is reasonable and can be demonstrably justified. In the Centre's view, the law should specify that information can only be collected for reasonable and demonstrably justified purposes. The Centre also suggests the legislation should contain the definitions of privacy and informational privacy specified in the Industry Canada and Justice Canada discussion paper.

Archivists/Historical/Library Associations

The Canadian Legislative and Regulatory Affairs Committee (CLARA) of the Association of Records Managers and Administrators (ARMA International) believes the "except where inappropriate" clause under Consent (*Principle 3*) of the CSA Standard gives too much discretion to information managers and is a potential area of dispute with consumers. CLARA also believes the requirement that information be retained only as long as necessary for the fulfillment of purposes (*Principle 5*) is overly vague since it does not clarify which purposes take precedence in determining an information retention period. Similarly, the phrase "required by law" may not adequately cover all situations. CLARA believes the requirements that individuals be informed of the existence, use and disclosure of personal information and be given access (*Principle 9*) are inappropriate as they go beyond the right of access embodied in the *Privacy Act* and equivalent provincial legislation, both of which establish specific exceptions to this right of access.

The Association des archivistes du Québec believes the law must allow society to maintain its "collective memory" by allowing the disclosure and use of personal information for research purposes, without consent, as allowed under the *Privacy Act* and the EU Directive — as long as this does not harm the individual involved. The legislation should also allow businesses to pass on personal information of historical value to any archive service without an individual's consent. The receiving organization should be obligated to destroy any personal information once it is no longer useful.

The Canadian Historical Association/Société historique du Canada (CHA/SHC) and the Institut d'histoire de l'Amérique française (Institut) believe legislation must recognize heritage issues, and are particularly concerned about building finality into data use, followed by

destruction. Both organizations state that legislation should not affect the ability of archives to collect, preserve and make available data collections to qualified researchers, nor should it limit the life of data necessary for historical research.

The Institut adds that legislation should set a time limit for the duration of information protection, specifically recognize personal data as also being archival material, and recognize the role of institutions and heritage organizations in maintaining this information.

The Ontario Library Association (OLA) wants legislation to be compliant with the *EU Directive*.

Telecommunications/Cable Sector

There were nine submissions from the federally regulated telecommunications and cable industries. These were: AT&T Canada Enterprises (AT&T); one collective submission by ACC TelEnterprises Inc., AT&T Canada Long Distance Services Company, Call Net Enterprises Inc., fONOROLA Inc., and Westel Telecommunications Ltd. (the AT&T Companies); the Cable Television Standards Foundation (CTSF); the Canadian Cable Television Association (CCTA); the Canadian Wireless Telecommunications Association (CWTA); Microcell Communications Inc. (Microcell); Rogers Communications Inc. (Rogers); Stentor Telecom Policy Inc. (Stentor) commenting on behalf of most Stentor and Mobility Canada companies; and TELUS.

Of these, only the CWTA and Microcell openly express support for legislation.

Nevertheless, all organizations state that the CSA Standard is the right starting point if legislation is to proceed, with all but one organization supporting the use of the Standard without further changes. Only Microcell suggests the wording of the CSA Standard needs to be more precise.

The AT&T Companies note, however, that the CRTC should receive direction from the Minister of Industry to delete the confidentiality of customer information provisions from the telecommunications carriers' Terms of Service, since they believe these provisions are inconsistent with the CSA Standard.

Stentor also adds that the legislation must provide for a transition period to allow companies to develop tailored codes and implement necessary practices to deal with both new and previously collected personal information.

Financial Sector

The financial sector contained submissions from both federally and provincially regulated organizations in banking, insurance services, securities regulators and stock exchanges, accountants, and organizations representing the interests of professionals who work within this broadly defined sector.

The Canadian Bankers Association (CBA) supports the proposed "light, flexible and effective" legislation based on the CSA Standard and says the Standard as it currently stands should be restated in the law in its entirety rather than being referenced. The Canadian Banking Ombudsman (CBO), however, does not support private sector privacy legislation, but believes the CSA model code should be recognized as a legislated standard for personal information protection, much as the generally accepted accounting principles (GAAP) are recognized as a compulsory industry standard with the effective weight of law.

Canada Trust and the Association of Canadian Financial Corporations (ACFC) support legislation based on the CSA Standard. ACFC states that sectoral codes are the most appropriate place to further detail obligations, while Canada Trust views further obligations as distorting the balance of interests. The Canadian Association of Financial Institutions in Insurance (CAFII) and the Canadian Life and Health Insurance Association (CLHIA) also support legislation based on the CSA Standard, without additional obligations. CAFII notes that the need for flexibility in obtaining consent must be recognized in the electronic age.

The Insurance Council of Canada (ICC) and Equifax Canada (Equifax) do not support legislation. ICC states that the property and casualty (P&C) industry does a good job with self-regulation. Equifax says there is no empirical evidence that voluntary codes have proven, or will prove, inadequate. Credit Union Central of Canada (Canadian Central) also prefers voluntary sectoral codes. However, all three organizations view the CSA Standard, as it now stands, as the right basis, if legislation is deemed necessary.

The Certified General Accountants Association of Ontario (CGA Ontario) supports legislation based on the CSA Standard, but adds that more detail is required. CGA Ontario suggests legislation should provide more specific guidance on consent for sensitive information and positive opt-out opportunities for non-essential information, along with more elaboration on when a subsequent use or disclosure of information would be consistent with original purposes and encompass original consent. CGA Ontario adds that the Access principle of the CSA Standard is vague on exemptions to the right of access, the time that may be taken, the fees that may be charged, and the circumstances when businesses may be required to provide personal information correction notices to third parties.

CGA Ontario also wants prohibitions on collecting and storing sensitive information such as political or religious opinions, trade union membership, race, health or sex life without legitimate need or appropriate safeguards, although collection of financial information required by business should not be so restricted. CGA further states that it should be an individual's decision whether personal information is used beyond the original purposes, and that new legislation should contain specific provisions on consent and the use of personal information for target marketing, data mining and other unrelated purposes.

Employees from Deloitte and Touche (Deloitte employees) also support CSA Standard-based legislation, but call for more specificity in the Safeguards and Openness principles. Under

Safeguards, broad references to technological measures should be augmented with a specific requirement to match the security level to the sensitivity of the information and to assess the viability of security measures on an ongoing basis. Deloitte employees also suggest organizations be required to match the methods of providing information about company privacy policies to the method of request, and that allowing organizations to mail responses to on-line requests directly conflicts with the purpose of setting out the Access principle in the face of emerging technologies.

A submission from Bennett Gold, Chartered Accountants does not deal with the substance of the Industry Canada discussion paper, but says that the CA WebTrust seal of assurance developed by the Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants should be adopted by the government as the audit and assurance component for electronic commerce in Canada. Bennett Gold states that trained and licensed chartered accountants should also be given the franchise for audit and assurance of electronic commerce and information protection.

Commercial/Retail Organizations

The Canadian Direct marketing Association (CDMA), Westcoast Energy/Enlogix Inc. (Enlogix), and the Sudbury and District Chamber of Commerce support legislation based on the CSA Standard with no further precision or obligations. Enlogix notes, however, that organizations should be required to publish complaints-handling experiences in summary form and retain records of complaints for audit purposes.

The Canadian Gas Association (CGA) opposes legislation, adding that any proposed legislation must avoid conflict with competition laws and should not set specific time limits for data retention or limit information use purposes. CGA notes the gas industry's requirements to collect and use customer data over a 20-year planning horizon. CGA also wants any legislation reviewed on a periodic basis (at least every five years), similar to sections 88 and 89 of the Québec *Act*.

Dun & Bradstreet Canada (D&B) raises concerns that the wording of the CSA Standard does not set clear and predictable rules, and is too restrictive in some areas. D&B notes that the CSA Standard is stricter than the *EU Directive* in limiting use or disclosure of information. D&B warns that overly restrictive rules would prevent disclosures of information, such as bankruptcy proceedings, that is of justifiable interest to the business community.

The Canadian Newspaper Association (CNA) expresses concerns about the CSA Standard in the context of journalism, as the organization feels the Standard creates onerous obligations on editorial processes, sets up uncertainty as to its scope and application in terms of media compliance, and undermines editorial independence. The CNA says legislation should be consistent with the *Universal Declaration of Human Rights* that guarantees the media's freedom of expression and its ability to "seek, receive and impart information and ideas."

Information Technology Associations

The Advanced Card Technology Association of Canada believes the CSA Standard is logical and easy to understand, but it should be compared with the EU Directive and provincial privacy codes and the strongest standard used. The Canadian Advanced Technology Association (CATA), the Canadian Association of Internet Providers (CAIP) and the Information Technology Association of Canada (ITAC) all support the CSA Standard without further changes. CAIP notes, however, that the law must clarify which parties are accountable for privacy law violations, stating that Internet Service Providers (ISPs) should not be liable for personal information disclosure by their customers or for inadvertent information disclosure of personal information as a result of cooperating with law enforcement agencies.

The Canadian Information Processing Society (CIPS) believes the CSA Standard should provide more guidance on intrusive data mining and computer matching, does not go far enough in specifying record-keeping requirements when data is disclosed to third parties, is silent on transborder data flow, and may allow implied consent to veil intrusive practices by marketers that, although not deceitful, are not fully informed.

Individuals (including consultants, experts and academics)

This question elicited considerable comment from the 22 individuals who responded. All individuals, except one, support the CSA Standard as the best place to start. No individual thought the CSA Standard was sufficient without changes. Changes suggested include:

- adding a principle of justification of collection;
- adding two principles from the proposed Charter of Privacy Rights from *Privacy: Where Do We Draw the Line?*, citing a duty to limit information collection to what is necessary and justifiable under the circumstances, and a duty not to disadvantage people because they elect to exercise their privacy rights;
- incorporating principles 6,7,8,10,17 and 18 from the Australian Privacy Charter. These principles address freedom from surveillance, privacy of communications, private space, anonymous transactions, public registers, and no disadvantage;
- incorporating the Telecommunications Privacy Principle that privacy invasive technologies be accompanied by policies that preserve privacy at no additional cost to consumers;
- reflecting the fair information practices of the Québec *Act*;
- adding a requirement to inform individuals about information management practices as well as means of redress;
- adding a requirement for agents or subsidiaries to grant access to information directly rather than through the main business;
- adding a requirement for businesses to inform individuals of their range of operations, agencies and subsidiaries;
- requiring businesses that share information with agents, subsidiaries or third parties to ensure information is as accurate as that provided by the main business;
- ensuring the law covers all information uses by individuals, businesses, agencies, not-for-profit groups, churches, unions, political action/interest groups and others;

- clarifying consent, with expanded requirements for explicit consent, and more limitation on the use of negative option consent;
- requiring all non-essential marketing uses to be tied to an opt-out opportunity;
- requiring parental consent for the collection and use of children's information;
- limiting information collection to the absolute minimum required (which would eliminate gratuitous information collection);
- specifying that information only be collected directly from the individual;
- specifying that indirect information collection be allowed only in the rarest of cases and always documented, except in law enforcement situations;
- setting a minimum retention period for any personal information (at least six months to one year after last usage);
- specifying that, when information is corrected, all information accidentally or wilfully obtained that is not vital to operations be deleted;
- where a business refuses to change, add or delete information, requiring a correction request to be attached to the contested information and a list of third parties provided to whom the information was disclosed in the past two years;
- adding a reference to applicable standards for secure custody and disposal of information;
- incorporating special protections and restrictions on the use of biometric data;
- establishing a right of self-determination of health records (based on the Supreme Court Decision in *McInerney v MacDonald*), with this right to be inalienable and to apply no matter where the information is held in order to place greater custodial responsibilities on organizations that maintain data banks;
- prohibiting collection of unique identifiers except where specifically and legally allowed;
- prohibiting the transfer of information to other countries without adequate protection;
- requiring a contract making the Canadian organization liable for disclosure of personal information outside of Canada;
- ensuring all information sharing technology and programs, along with their purposes, are approved by government;
- requiring businesses providing services to government to be subject to the same obligations as the government body, and to public sector privacy laws;
- providing protection from fees and charges that could frustrate timely access to personal information;
- prohibiting eavesdropping and interception of information without the consent of both parties or a court authorization;
- requiring organizations to provide free summary listings of personal information used to provide services or make decisions, along with a fee structure to reflect the actual costs of providing full access;
- prohibiting surveillance except for law enforcement purposes;
- extending the same legal protections to e-mail as voice telecommunications;
- making it a violation similar to mail fraud to send SPAM (unsolicited junk e-mails) to people who don't want it;

- facilitating privacy protection through public key encryption to prevent mail-header forgery.

Highlights

It is generally agreed that the CSA Standard should be the basis for legislation. However, comments by various parties, including privacy commissioners, consumer groups, business organizations, special interest groups and individuals, on the need for greater precision and additional obligations should be considered in any drafting exercise.

2. Under what circumstances should the law permit disclosure of personal information to a third party without the consent of the individual? What conditions should apply?

Most parties who commented on this question feel the law should allow disclosure of personal information without consent for law enforcement as well as medical emergencies and other limited compelling circumstances when people are incapable of supplying their own information. Included in this category are cases of peril to health or safety, threats to others or self-injury, or where absolutely essential for business purposes (e.g. in cases, such as described by telephone companies, when personal information needs to be disclosed to ensure the effective operation of telecommunications networks). Risk to the environment is also suggested by the Information and Privacy Commissioner of Alberta and by one other party as a legitimate reason to allow disclosure without consent.

The use of personal data for medical research purposes elicited responses that disclosure without consent should occur only where there is a direct benefit to the individual or a clear "public good" as in research uses, with person-specific information available only where there is a direct benefit to the individual. There is little support for disclosure of personally identifiable health information without consent, except in rare circumstances. There is support for the idea that every disclosure for research purposes or in the public interest should require express individual or oversight body approval.

The archival community wants a carefully delineated exemption from consent requirements for historical material, while the Canadian Newspaper Association advanced strong views on the necessity for disclosure without consent for journalistic material.

Within the private business sector, many respondents feel the current wording within the CSA Standard is sufficient. Others want more clarity to deal with a number of specific situations, such as the collection and prevention of debt and, in the case of telephone companies, for business purposes such as customer win-backs.

Cable companies and ISPs want exemption from liability under the legislation when information is disclosed by a member of the public using their facilities, and when the information is not under their direct control.

Businesses that collect and use publicly available and business-related information about individuals want this information subject to disclosure without consent, saying it is often in the public interest to do so (e.g. there is a public interest in disclosing information concerning situations such as bankruptcy proceedings), while regulatory agencies such as securities regulators also want to collect and use information without consent to protect the integrity of the financial markets.

The insurance industry mentioned public duty responsibilities to disclose information without consent where the data is useful to public authorities to meet public objectives.

In contrast to these various examples, consumer groups generally want strict limits placed on disclosure without consent. There is only mixed support for disclosure without consent for journalistic purposes. The suggestion was also made that organizations be required to document and justify any disclosures without consent. Some of the varying positions are outlined below.

Privacy Commissioners

The federal Privacy Commissioner states disclosure without consent should only be allowed if the health and safety of the individual is at risk, or if required by law.

The Information and Privacy Commissioner of Alberta suggests disclosure without consent be allowed for law enforcement, for the health and safety of an individual, and for information about a risk to the environment, the health or safety of the public and when disclosure is clearly in the public interest.

Both the BC and Ontario Commissioners favour narrow and clearly defined circumstances for disclosure without consent. The Commission d'accès prefers the wording of the Québec *Act*.

Consumer Groups (including organized labour)

All groups that commented on this issue state that personal information should hardly ever be released without consent, citing law enforcement, emergencies and cases of peril to health or safety as the only grounds, based on an explicit, narrow and clearly defined public interest override. FIPA adds that specific probability of harm should be demonstrated.

PIAC adds that the law must also address the disclosure without consent of information in the public domain.

Health Care Sector

The CDA believes the law must allow disclosure without consent in specific health cases where a health practitioner has reason to believe the actions of a patient may cause harm (e.g. when dealing with patients with sexually transmittable diseases). In such cases, only the data specifically required should be released.

The CNA believes disclosure without consent should occur only where there is a direct benefit to the individual or a clear public good as in research uses, with person-specific information disclosed without consent only where there is a direct benefit to the individual. CIHI states that person-specific data should not be disclosed without consent except in specially defined situations. IMS believes no attempts to define exceptional circumstances would be comprehensive and wants the term "where appropriate" to be retained in *Principle 3* and added to *Principles 4 &* 5 of the CSA Standard.

Law Enforcement

The RCMP believes disclosure should require informed consent or that, at a minimum, individuals should be made aware that their information may be disclosed under specific and limited circumstances.

The RCMP adds that the legislative framework must allow disclosure to law enforcement agencies or other government investigative agencies (e.g. Customs, the Competition Bureau and Revenue Canada) based on Section 8 (e) of the current federal *Privacy Act* which permits disclosure without consent to "an investigative body specified in the regulations on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed."

Institutes

The U of O Centre recommends that the definition of consent include a statement that everyone has an inalienable right of ownership to their personal information, no matter where it is held.

Archivists/Historical/Library Associations

The Association des archivistes du Québec recommends a stipulation that consent be obtained for the use of sensitive personal information for a period of 20 years from the date of a document, extending to 75 years for sensitive personal information. Upon expiry of this period, individuals could also seek written authorization to keep personal information as personal property for a maximum period of 100 years from the date of the document.

CLARA recommends that guidelines for disclosure without consent follow those of the *Ontario Freedom of Information and Protection of Privacy Act* and the federal *Privacy Act*. The OLA wants disclosure without consent limited to specific scenarios such as threats to personal health and safety or when data has been stripped of all personal identity links.

The CHA/SHC believes disclosure without consent should address historical access to personal information about deceased persons, while the Institut d'histoire de l'Amérique française views the actions of obtaining consent, limiting the collection, use, retention and disclosure of personal information, and implementing security measures, accessibility and correction opportunities as being in direct contradiction to the activities related to history.

Telecommunications/Cable Sector

AT&T suggests that notifying individuals or seeking consent for disclosure should not be required in every telephone company transaction. The AT&T Companies expand on this by saying rules for disclosure without consent should follow generally accepted circumstances as indicated in the Québec *Act*, the federal *Privacy Act*, the *Telecommunications Act*, and current sectoral codes such as that of the Canadian Bankers Association. Sector-specific exemptions should be permitted, proposals for which should be registered with the federal Privacy

Commissioner. The AT&T Companies also suggest that telecommunications companies be allowed to share information about their customers without consent in case of emergency, and in the case of individuals who are in a debt situation (to prevent these individuals from running up large debts with more than one company). The AT&T Companies add that information sought pursuant to a legal power should not require consent and that legislation should take into consideration different business situations when defining the right to withdraw consent. The AT&T Companies view use and disclosure of personal information for purposes such as customer win-backs as legitimate business purposes which should not require further consent.

Microcell adds that disclosure without consent should be allowed to protect health and safety, for law enforcement, to protect against customer fraud, and to ensure that interconnected networks can operate efficiently. The CWTA position generally concurs with the Microcell view, adding that disclosure without consent should also be allowed where a third party, in the reasonable view of a service provider, is seeking personal information as an agent of the subscriber.

The CCTA notes that companies cannot be held liable for collection, use and disclosure of personal information by a member of the public involving the use of communications services and facilities provided by cable companies, where cable companies do not have direct control over the information. Rogers generally supports all of the positions stated above.

Financial Sector

CBA lists a number of specific situations where disclosure without consent should be allowed, including fraud, forgery, law enforcement, when the individual is a minor, seriously ill or mentally incapacitated, and cases where the data holder has an agent relationship with the third party providing related services. In these cases, a contract would be required to protect the personal information given to the third party. The CBO suggests disclosure without consent should be as per the current CSA Standard.

ACFC, Canada Trust, CLHIA, Equifax and ICC all support disclosure without consent as per the current CSA Standard. Canada Trust believes a sectoral code is the most appropriate place to provide more detail on disclosure without consent, and notes that disclosure without consent is required for agent relationships with third parties providing related services. ICC states that "public duty" should be added to the list, citing the nature of the relationship between P&C insurers and provincial motor vehicle registries that leads to the sharing of some information (e.g. claims-related data where there is a public interest) that is not strictly a legal requirement.

The Canadian Securities Commission, Canadian Securities Administrators and the Vancouver Stock Exchange (VSE) state that securities regulators need to be able to collect, use and disclose personal information without consent to carry out their mandate, which includes investigation of industry participants. The VSE calls for an exemption from legislation for the collection of information about members and listed companies, stating that individual access to this information should be denied in order to maintain public confidence in the integrity of

securities markets.

CGA Ontario says legislation should provide a short list of exceptional situations for disclosure without consent that would include disclosure with a search warrant or subpoena, if the information is already public, in the case of an emergency threatening health or security, and for legitimate research purposes where the information will not be disclosed to the public in a way that identifies the individual.

Commercial/Retail Organizations

Enlogix supports enumeration of circumstances as per the Industry Canada discussion paper. D&B believes strict limitations on disclosure without consent should only exist where information is normally considered confidential, noting that a great deal of information is by nature public and should be subject to legitimate public communication without consent. D&B notes that such public disclosure is essential in securities transactions and should be allowed in other cases where legitimate third party interests exist.

The CNA dismisses as ludicrous the concept that only those stories can be published wherein the subjects are pleased to consent to disclosure. CNA states that a clear exemption for journalistic purposes is required as use of the "except where inappropriate" clause in the CSA Standard (*Principle 3*) would only invite litigation.

Information Technology Associations

CAIP believes information should be disclosed without consent when there is a threat of self injury or a threat to others, with disclosure limited to a need-to-know basis. CAIP also states that a user policy or executed contract permitting disclosure without consent constitutes consent and should be recognized by law. CIPS would limit disclosure without consent to limited compassionate or compelling circumstances or situations where an organization is explicitly bound by law to disclose information. CIPS suggests disclosure without consent in law enforcement not include cases where law enforcement agencies are investigating their own employees. As well, private investigators should not be allowed to rely on legal provisions to seek disclosure without consent. CIPS also believes that, if disclosure of personal information without consent is to be an offense, it should also be an offence to attempt to gain access to such information without consent.

Individuals (including consultants, experts and academics)

Individuals had a number of suggestions on when disclosure without consent should be allowed, including:

- the current *Privacy Act*, section 8 (2) items *A* to *M* is a good starting point for a list, with a caveat that individuals be notified whenever there is disclosure without their knowledge and consent;
- the list should be more limited than the current *Privacy Act*, and disclosures without consent under court orders or judicial warrants should be brought to the attention of

the affected individual;

- disclosures for research, audit or statistical purposes should be allowed with approval from the federal Privacy Commissioner;
- disclosure without consent should only be when allowed by law in circumstances such as wiretaps;
- circumstances should be specifically delineated and indicate the benefit to the individual or the wider public interest;
- disclosure should be allowed where absolutely necessary in the operation of a business, with every disclosure logged;
- consent should always be required except in compelling circumstances such as danger to health or the safety of people, including environmental hazards (it was noted that, in order to protect privacy, health practitioners should not disclose an entire patient file when they are required to disclose patient information under law, such as knowledge of sexually transmittable diseases);
- disclosure without consent should be allowed by the media for news purposes;
- no one should be able to read e-mail without consent except by court order, and private companies should be required to inform employees when corporate e-mail is being monitored;
- an individual's rights to privacy should not be absolute and the community should have overriding rights to disclose information in instances such as addictive behaviour that disrupts a community.

Highlights

Various business organizations and other parties suggested specific categories of information use that should be subject to disclosure without consent. Other parties, including privacy commissioners and consumer groups want an extremely limited and highly specific list of information use categories and situations where disclosure without consent would be allowed. It was also noted by some parties that no such list can be exhaustive. In light of these differing positions, the best approach may be to include a well delineated list of examples of disclosure without consent within the legislation, and provide further guidance on circumstances under which such disclosures would normally be allowed. The suggestion made by a few parties that organizations be required to document and substantiate any such disclosures without consent is also worth consideration.

3. Should sectoral codes be recognized in the new law? If so, should they be binding? Or should they be used only to help interpret the principles of the law for specific sectors? Who should develop and approve them?

Many submissions acknowledged the value of sectoral and organizational codes in helping industry groups to interpret the CSA Standard. However, there was only limited support for binding sectoral codes under the law, especially for codes that would replace the legislation.

There were a few parties who would give sectoral codes legal weight by virtue of a government approval process. IMS Canada, the Canadian Dental Association, the Canadian Banking Ombudsman and the Canadian Direct Marketing Association all support legislated sectoral codes for all industry sectors and a national certification system. The Insurance Council of Canada wants sectoral codes to be binding on industry sectors and wants industry codes, therefore, recognized in law as having interpretative value when cases of non-compliance arise. Interpretative value means that in resolving disputes, setting penalties or awarding compensation, an oversight body must give due consideration to the organization's code and the manner in which this code was applied in determining if the law was violated.

The Public Interest Advocacy Centre suggests, however, that if sectoral codes do have any legal weight, they must at least meet, if not exceed the legislation, apply to an entire clearly defined sector, and be subject to public input.

The clear majority view is not supportive of binding sectoral codes replacing legislation or having recognized legal weight.

The positions of the various parties are outlined below.

Privacy Commissioners

Only the Information and Privacy Commissioner of Ontario supports the recognition of sectoral codes in the law. The Commission d'accès notes that no provisions exist for recognizing sectoral codes within the Québec *Act*.

The Ontario Commissioner states that sectoral codes should be recognized in law and binding as per the New Zealand model, noting, however, that the need for such codes will be quite limited if the legislation is well written. Binding sectoral codes should be reviewed by a number of parties including the responsible Minister, the oversight agency and an industry committee before being approved. The Commissioner warns, however, against ratification or grandfathering of existing sectoral codes developed before the presence of a law.

Consumer Groups (including organized labour)

Most consumer groups, including FIPA, BCOAPO, CAC, PIAC and Privacy Partners, along with CUPE, support the use of sectoral codes only as non-binding, interpretative documents.

CAC Ontario says such codes could be approved for use by the federal Privacy Commissioner but should not take precedence over legislation. BCCLA supports their use, providing there is funding for public interest participation in their development and consensus-based decision making. BCCLA believes such codes should have some official stamp of recognition indicating the development process was fair and inclusive, but not the authority of law.

FNACQ/OC sees such codes as being effective only if they are legally binding, and proposes that industry develop codes but the federal Privacy Commissioner verify them to ensure compliance with the law.

PIAC states that, if binding codes are allowed, they must equal if not exceed the legislation, should apply to an entire clearly defined sector, and the process to approve and enforce codes must include public input.

Health Care Sector

The CDA supports sectoral codes being recognized in law, as the organization believes specific privacy threats from corporate mergers, a variety of information gathering techniques and target marketing practices are too great to be left to self regulation. CIHI and IMS also want sectoral codes recognized in law. CIHI says they should be approved by groups knowledgeable about the sector and privacy laws. IMS states such codes should be certified and binding in the same way that adherence to the law is binding.

The CNA does not support the recognition of sectoral codes as a substitute for legislation.

Government (including the European Union)

The EU believes voluntary, non-binding codes are useful but less effective in isolation and more costly to implement and enforce.

Archivists/Historical/Library Associations

CLARA supports the use of sectoral codes as non-binding guides for tailoring the law and urges Industry Canada to encourage industry to include these codes in the National Library depository system, to make them accessible to the public. The CHA/SHC believes sectoral codes might be acceptable if they included far-sighted management policies. The OLA advocates the recognition of sectoral codes as binding where there is agreement among all stakeholders. OLA states that the proposed legislation, however, should supercede any sectoral code.

Telecommunications/Cable Sector

All respondents except AT&T support non-binding sectoral codes, developed and used for interpretation only. AT&T believes the government should outline requirements for codes which would then be developed by industry for review by the oversight authority. These codes would then be binding on the industries to which they apply.

Financial Sector

The CBA, CBO, CLHIA, Equifax, Deloitte employees and Canada Trust all support use of non-binding, interpretative sectoral codes, with Canada Trust suggesting that a reference to the role of sectoral codes be included in legislation. CLHIA does not support this last point, while Equifax states that legally binding provisions could be subsequently enacted if voluntary compliance proves to be demonstrably inadequate.

Only two organizations, ACFC and ICC advocate specific recognition for the interpretative value of sectoral codes in law. ACFC prefers a recognition of the interpretative value of codes that are non-binding. In this case, industry sectors would be required to develop and adopt codes, but approval under the law would not be required.

ICC also believes sectoral codes should be developed by the sector, without government involvement, but they should be certified by accredited independent auditors and registrars. They should then be recognized in law as binding on the industry sector. ICC states that codes recognized in law as binding on an industry will lead to greater certainty and predictability in how oversight is applied.

CGA Ontario favours the New Zealand model, under which binding industry codes require public sector input and federal Privacy Commissioner approval, with some method for the Privacy Commissioner to require their review and revision if circumstances warrant.

Commercial/Retail Organizations

The CDMA believes sectoral codes should be registered with a national body and certified as meeting the CSA Standard, while D&B suggests, based on the limited industry experience with voluntary codes, that it is premature to judge how sectoral codes should be integrated into legislation. Enlogix does not think sectoral codes should be binding, and the CGA sees no need for sectoral codes or guidelines within the natural gas industry.

Information Technology Associations

All organizations in this sector support non-binding sectoral codes, used for interpretation and guidance only.

Individuals (including consultants, experts and academics)

Individual opinion on the value of sectoral codes ranges from no support at all (a "waste of time") to a view that they should be non-binding and used for interpretation only.

Only two individuals believed sectoral codes should have any formal recognition. One health care practitioner said they should be recognized in law where groups such as medical ethics committees must regulate over professional bodies to protect the public, and exercise powers to sanction members and assess penalties. Another individual said they should be developed by industry and associations and verified by recognized professional bodies.

Highlights

There is limited support for binding sectoral codes, and it is generally suggested by respondents that there be no provision within legislation to allow sectoral codes to replace legislation or have legal recognition, including interpretative value. One business submission, in particular, raised the issue of the interpretative value of such codes (i.e. courts, in determining penalties or awards would have to give due consideration to the manner in which the organization interpreted the legislation within its sectoral code). One consumer submission, however, suggested that a fundamental reason why greater precision is required within the legislation is to prevent organizations from using the "impenetrable defense" that they have applied subjective judgement to the CSA Standard in good faith. Perhaps, given these conflicting views, the question of interpretative value is best left to the courts without any direction within legislation.

4. Should some types of information be excluded from the scope of legislation? If so, in what circumstances?

This question elicited specific and detailed comments from only a few respondents. The federal Privacy Commissioner and the Alberta Commissioner do not want any exclusions while the BC Commissioner wants the law tightened even further to include biological information such as tissue samples. There are mixed views on journalistic exclusions.

Among others who commented on this question, there was mixed support for completely excluding journalistic material. One individual suggestion was that this issue be dealt with similarly to the EU Directive which excludes such material from some provisions of the Directive, but not all.

There were also suggestions that information of an entirely personal and non-commercial nature (e.g. a personal telephone directory or photo album) should be excluded.

One suggestion worth highlighting is that the definition of "person" under the law should extend to "natural persons" only, so as not to convey privacy rights to corporations.

There were mixed concerns about how far information already in the public domain should be excluded (if at all) since there are notable differences between widely available public domain information and information that, while available, is generally not intended for widespread distribution or use. As described below, there are also many other noteworthy exclusions sought by business organizations.

Privacy Commissioners

Privacy commissioners generally believe there should be no exclusions or they should be extremely limited. The Information and Privacy Commissioner for BC believes the range of information subject to the legislation should be extended to capture biological information such as tissue samples. The Information and Privacy Commissioner of Alberta does not advocate excluding any information and the Information and Privacy Commissioner of Ontario does not advocate exclusion of journalistic material. The Commission d'accès does support excluding the collection, retention, use and disclosure of personal information for journalistic purposes as per the Québec *Act*.

Consumer Groups (including organized labour)

This question was only directly responded to by three organizations, with the focus largely on journalistic material. The CAC opposes any exemptions, including for information collected and used for journalistic purposes. FNACQ/OC believes journalistic material should be exempt as per the Québec *Act*. FNACQ/OC also believes information used for artistic purposes should only be exempt where the individual involved could not reasonably expect protection and where all efforts have been made to obtain consent. FIPA believes exemptions should exist for journalistic material, and judicial and ecclesiastical records, as well as

information compiled and used for purely personal purposes. FIPA adds that personal information in archival material could have a carefully delineated and limited exemption.

Health Care Sector

Both CIHI and IMS Canada want non-identifiable data excluded from the law.

Government (including the European Union)

The EU cautions that it has not found it wise to exclude certain types of data processing entirely from the scope of legislation. In their view, a more appropriate balance would be to exempt data processing activities such as journalism from certain principles.

Archivists/Historical/Library Associations

The Association des archivistes du Québec believes that files and documents of a personal nature that are stored manually are naturally protected and, therefore, should be exempt from legislation as long as the information is not collected specifically on an individual and the document is not computerized. The CHA/SHC also urges exemption of data of a historical nature, while the OLA wants all data to be exempt where links to individuals have been removed.

Telecommunications/Cable Sector

The CWTA believes there should be no exemptions while Microcell would exclude journalistic material and suggests there may be a need to exclude information used to ensure the security of public key-based encryption systems.

The AT&T Companies believe that, within the telecommunications sector, companies acting in the role of a carrier or service provider should be exempt from any accountability for the use made of communications facilities by customers. Legislation should not require businesses to seek to gain control of or to protect information not under their control by virtue of the products and services they provide. Rogers supports this position and adds that information not attributable to an identifiable individual be exempt, such as information traceable only to an Internet protocol (IP) address, not an individual. Similarly, Rogers would exempt Internet usage information compiled in aggregate form which may be used for marketing purposes.

Financial Sector

CBA states that the scope of legislation should be limited to information about natural persons, and that proprietary information should be excluded so as not to jeopardize the competitive positioning of business organizations. CHLIA favours exclusions as per the current CSA Standard. ICC proposes that information about non-identifiable individuals be exempted.

The Western Forum of Credit & Financial Executives cites the requirement for credit agencies to retain information for long periods of time in order to combat the misuse of credit and credit fraud. The Forum adds that overly broad definitions of personal information in the CSA Standard coupled with onerous consent requirements could lead to censorship of data under

the guise of privacy protection, with harmful effects to the credit industry. The Forum, therefore, calls for personal information now governed by provincial credit reporting, debt collection and other related legislation to be exempted from privacy legislation, as well as information used for the initiation, extension and collection of credit. The Forum adds that information for business contact purposes should be exempted and record-keeping for ongoing business purposes should be considered the private property of the firm lawfully obtaining the data.

Equifax also proposes exemption of consumer credit information since it is already subject to provincial laws, stressing that such an exemption is particularly necessary if harmonization of various jurisdictions cannot be achieved.

Commercial/Retail Organizations

Enlogix advocates that all statistical or aggregated data be excluded from the scope of legislation if it cannot be rendered personal again through manipulation. D&B believes information gathered about business entities should be excluded from legislation and that the legislation should apply only to natural persons.

The CNA believes information gathering for the purposes of journalism and newspaper archival material should be exempted from the scope of legislation to protect constitutional values.

Information Technology Associations

CAIP states that the same conventions that apply to other forms of communications should apply to e-mail, and any party who legitimately receives personal electronic messages should be able to reveal the contents and any electronic header information (i.e. Internet Protocol addresses) without fear of reprisal. CAIP also believes on-line businesses should not be regulated more than other commercial enterprises and, thus, ISPs (only some of which may be subject to federal privacy legislation) should be able to use subscriber electronic header information for marketing purposes, and to rent and sell to other organizations, much as magazine publishers do with subscriber lists.

CIPS is concerned about treatment of records within the public domain and questions whether any exclusion of such records should apply to individual records only or an entire database. CIPS also believes legislation needs to address whether an organization can use a public record for purposes other than those for which it was originally compiled. Also at issue is whether organizations should be able to use public records created for one regulatory purpose to fulfil another regulatory purpose.

Individuals (including consultants, experts and academics)

Eight individuals commented directly on this question and their comments reflect both general and specific concerns about exclusions. One individual states there should be no exclusions; another wants no exemptions that would relieve business of the legal responsibility to protect customer and employee privacy. Another individual adds that the law should apply

equally to employee and customer information, and employees should not be required to sign away privacy rights with waivers in employment contracts. However, a contrary view from one health care practitioner is that organizations that use limited amounts of data should be allowed to register and define how they would apply the CSA Standard (e.g. be exempt from legislation), while institutions that collect and use a great deal of personal information would be subject to a specific, enforceable law.

Another health practitioner believes groups such as researchers should be able to apply for an exemption from subpoena for any particular research information and wants information such as cancer registries, Statistics Canada mortality and morbidity files, and hospital admission and separation files treated in a different context than private sector business information.

One individual states that data that has been rendered anonymous should be excluded and freedom of the press needs safeguarding. This was supported by one journalist who adds that the law should apply only to organizations, not natural persons (including free-lance journalists). Another individual opposes exclusion for journalistic material, but states that information about any individual who has been deceased for two years, information for strictly private and non-commercial uses, and information from widely known and accessible sources such as telephone directories should be excluded.

Highlights

The submissions indicate that the legislation should define "person" to include only natural persons to avoid giving organizations the information protection rights of individuals. The drafters of legislation should also consider whether to distinguish between widely available public domain information and public information that is not intended for widespread distribution or use. Where categories of data users seek exemptions from the legislation, the drafters should consider whether to exempt users from the full scope of the legislation or whether exemptions, if any, should be restricted to particular aspects (e.g. an exemption from the obligation to obtain consent before information collection, use or disclosure).

Powers

5. Do you favour start-up obligations such as a registration scheme to ensure compliance with the law? If so, which approach do you favour? Who should be responsible for overseeing privacy protection?

The majority of respondents see little value in or are opposed to complex registration schemes. No privacy commissioners support the concept as do few business respondents. There is limited support for the mandatory filing of codes and contact information with the federal Privacy Commissioner or other public body. This view is supported by the AT&T Companies, Stentor, and the Association of Canadian Financial Corporations.

Most consumer groups, however, do support start-up registration of some type, as do two individuals. The main purpose and support for such registrations is generally to establish a central repository of codes and contact individuals. Specific views are outlined below.

Privacy Commissioners

Privacy commissioners are unanimously opposed to start-up obligations such as registration, calling such regimes cumbersome and expensive, unnecessarily bureaucratic and possibly counterproductive. In general terms they note that since data commissioners around the world have frequently been tasked with running registration systems, this community is well placed to comment on the effectiveness of such schemes.

Consumer Groups (including organized labour)

Of eight consumer groups that responded to this question, three oppose mandatory start-up registration and five support it.

Privacy Partners supports it, but says the process should not be onerous for non-profit organizations and small business, but should instead lead to easy access to information on organizational practices and policies. PIAC says registration will help identify "high risk" data users, as well as identifying and monitoring inappropriate and inadequate practices. The registry should be maintained by the oversight body which should have the resources to properly review filings and conduct follow-up activities ranging from phone calls to full audits. A registration fee would help fund the oversight body's education and oversight activities. All companies that deal with personal information would also have to report annually and make public information on complaints handling.

CCC and CAC Ontario also support registration, as does CAC which calls for registration schemes suitable for the size of the business and the sensitivity of the information, with third party verification by Standards Council of Canada (SCC) accredited privacy registrars as the norm. The legislation should specify when self-registration would be allowed, such as for small businesses or for non-sensitive information.

Health Care Sector

Only CDA supports mandatory registration, adding that some sectors dealing with vast amounts of personal information may require specific enforceable legislation. CIHI suggests registration with the CSA or the federal Privacy Commissioner could be voluntary.

Archivists/Historical/Library Associations

Neither CLARA nor the OLA support a start-up registration scheme. Other organizations are silent on this issue.

Telecommunications/Cable Sector

There are only two comments in support of any form of registration. The AT&T Companies support registration of sectoral codes with an oversight body, as well as providing the name of the organizational contact responsible for administering codes. Stentor believes registration can be useful, but companies should be free to employ it where they see fit. Stentor also suggests that tailored codes, along with the name of the contact person, could be filed online with a government web site.

Financial Sector

Most respondents who commented on this issue do not support start-up obligations or registration. ICC suggests compliance to a code should be assumed in the absence of complaints or any compelling evidence to suggest a problem with personal information protection. CBO states that, in order to support its model of maximum industry self-regulation, codes should be audited by accredited privacy examiners.

ACFC suggests a requirement to file codes with the federal Privacy Commissioner, which it deems to be a cost-effective alternative to registration. Equifax states it is not opposed to voluntary registration and suggests such schemes could become compulsory if there is evidence of a high level of non-compliance.

Only Deloitte employees support start-up registration with initial audits. Audit results would be reported back to a sectoral body and passed on to an oversight agency for monitoring. The sectoral body should periodically review privacy policies to ensure they remain current in a changing technological climate.

Commercial/Retail Organizations

Enlogix favours start-up registration, with tailored codes approved by an accredited body under the SCC or a government body under legislation. Industry should develop such codes with CSA or government guidance. Any initial or subsequent audits should be performed by accredited third-party auditors, not government, and should not be mandatory.

The CDMA also supports registration of codes. The CGA, however, is opposed to registration and states that, if a registration scheme proceeds, utility companies should be exempt

to reduce regulatory burden. The CGA also believes federal privacy law would be an intrusion into property and civil rights matters constitutionally under provincial jurisdiction.

Information Technology Associations

No organizations support start-up obligations such as registration. CIPS supports a "self-declaration of compliance" which is subject to challenge by third parties and review by the oversight body. In return for self-policing ability, companies should be required to keep rigorous records to demonstrate compliance.

Individuals (including consultants, experts and academics)

Seven individuals commented on this question, of which four do not support start-up obligations. Of the rest who support them, one wants a privacy registry data base where mandatory registrations could be self-filed and publicly available via the world wide web. Another suggests voluntary registrations may serve as evidence of compliance with the law and would, therefore, minimize the amount of verification or auditing necessary by the federal Privacy Commissioner.

One individual suggests businesses planning to use intrusive technologies such as biometric identification or smart cards should be required to register or be licensed by government.

Highlights

Support for registration procedures, where it exists, seems to be on the merits of creating a central repository of codes and contact individuals. Given the lack of support for this concept from privacy commissioners, and the availability of such information directly from organizations under the law, a registration process appears to be unnecessary.

6. What powers are needed to investigate cases of non-compliance and resolve disputes about the terms of compliance?

Generally, all parties commenting on this issue recognize the need for investigative powers when a complaint arises. However, not all parties provide a detailed listing of those powers required to conduct an investigation. Where detailed powers are mentioned, they are generally in line with the existing powers of the Privacy Commissioner. Specific comments are outlined below.

Privacy Commissioners

The federal Privacy Commissioner lists existing powers under the current *Privacy Act* along with additional powers, including the ability to impose fines if investigations are wilfully obstructed, a power to refuse to investigate or to abandon a complaint under certain circumstances, and a power to initiate and receive complaints directly. Powers are also required to approve and monitor disclosure of personal information for research and statistical purposes.

The Information and Privacy Commissioner of Alberta believes the oversight body must have powers to respond to complaints and investigate on its own initiative, have full rights of entry and access to information, audit records and information management systems, mediate disputes, set deadlines for response, hold hearings, examine witnesses, issue binding orders, and impose penalties for wilful obstruction. The oversight body should also be able to comment on the privacy implications of new technologies, services or programs, and oversight agency personnel should be protected from proceedings while performing legislated functions.

The Information and Privacy Commissioner for BC believes the powers should be those of the existing federal *Privacy Act*, with the necessary regulatory powers to settle disputes that proceed beyond industry dispute resolution procedures. The Information and Privacy Commissioner of Ontario lists a full range of powers similar to those listed by the Alberta Commissioner, with the addition of powers to issue binding orders with full and effective remedies.

The Commission d'accès recommends powers as per the Québec *Act*.

Consumer Groups (including organized labour)

CPI recommends a complaints-driven model only, in which consumers and business are both made aware of their rights and obligations. If consumers are not satisfied with the outcome of their complaints to business, then an independent investigation can take place. All investigation reports from the oversight body should be publicly available from the organization being investigated, similar to a Better Business Bureau approach to customer satisfaction.

All other consumer organizations support more proactive investigative powers. FIPA suggests powers similar to those found in provincial privacy legislation. PIAC details the fullest range of powers of all responses. In addition to powers already noted, these include: the power to

make all investigation and audit results public; express legislative powers to delegate certain investigative/audit functions to qualified third parties; the power to make industry regulations governing practices and procedures; the power to charge fees to data users; the power to impose penalties for non-compliance and issue remedial orders. PIAC adds that individuals should also be able to require mandatory investigation by the oversight body based on the six adult person threshold established under S.9 of the *Competition Act*.

Health Care Sector

IMS Canada says the law requires powers to demand periodic internal or external audits, and the CDA calls for powers to review, audit and discipline.

Government (including the European Union)

The EU suggests an independent oversight authority must have powers to verify compliance with the law even in the absence of complaints.

Institutes

The U of O Centre believes privacy commissioners should have powers to receive, investigate and settle complaints of alleged privacy violations.

Archivists/Historical/Library Associations

CLARA believes powers should be consistent with those of the Information and Privacy Commissioner of Ontario and include the powers to investigate non-compliance, obtain copies of records, require information to be submitted under oath, and both issue and publish recommendations to improve compliance and conduct follow-up investigations.

The OLA suggests organizations deal with complaints first and be required to report the complaint and the resolution to the federal Privacy Commissioner. The Privacy Commissioner's powers should be limited to the investigation of actual violations.

Telecommunications/Cable Sector

The AT&T Companies suggest the oversight body should be restricted to receiving complaints and should rely on self-regulatory organizations to resolve these complaints, while monitoring compliance and undertaking investigations and research as required. There should be a statutory duty to meet with and mediate between parties to any given dispute.

Stentor also supports a complaints-driven process in which companies and individuals attempt to resolve disputes first, with the oversight body having powers to investigate disputes, mediate between parties and make recommendations for improving practices where disputes cannot be resolved directly between the parties.

The CWTA concurs with this approach and adds the legislation must clearly indicate the principles to be respected in investigating any alleged privacy violation. The CWTA says that

any decisions arising from investigations should be accompanied by reasons for a decision, and proper legal procedures must be followed to gather information.

The CCTA and Rogers, which favour continuing oversight by the CRTC, state that the current CRTC powers to inquire into matters, hear evidence, determine facts and make mandatory decisions are sufficient to protect personal information.

Financial Sector

CBA and the CBO believe the primary responsibility for privacy oversight must rest with sectoral organizations. CBO says that, where industry-managed sectoral bodies exist, the sectoral oversight body should only make non-binding recommendations to the dispute parties when disputes cannot be resolved. The sectoral oversight body should, however, be required under legislation to report publicly on complaints received and how they were resolved. CBO believes that the threat of such public reporting should be a sufficiently persuasive mechanism to make any recalcitrant business follow the recommendations.

Canada Trust and Equifax also suggest the greatest reliance should be placed on industry-led mechanisms. Canada Trust says the powers of an oversight body should include a role of policy advisor, as well as reviewing company codes and processes in the infrequent cases where issues remain unresolved.

Equifax calls for limited investigative powers and no proactive inspection powers. The oversight body should be required to refer all complaints first to the business or entity involved, with subsequent power to refer complaints to provincial oversight agencies where entities are subject to provincial jurisdiction. Only when all such processes are exhausted should an individual have the right to appeal to a national oversight body.

ICC supports oversight powers to conduct investigations and inspections where appropriate, but with clear limits. In ICC's view, in the absence of a complaint, investigation should only be authorized where there are reasonable grounds to believe the law is being breached. ICC also states that current federal Privacy Commissioner powers suitable for the public sector, including powers to publicize findings, could lead to well-intended but wrong orders with severe and unintended consequences for P&C insurers.

CGA Ontario calls for broad powers of enforcement, including the power to audit information use practices, to make specific orders pertaining to a business and general orders pertaining to broader, industry-wide problems. Legislation should specify that these latter powers be used only in exceptional circumstances, and industry should be able to apply for some form of judicial review for both specific and general orders.

Deloitte employees favour powers provided within a legal framework for sectoral oversight bodies, such as industry associations, to demand third-party audits and investigations, including examining witnesses, requiring testimony, ordering the production of documents and

arbitrating decisions. The results of this audit process could be appealed by the complainant to the sectoral oversight bodies or a government legislated oversight body, whose decisions would be binding. Violations of the code should be publicized as an incentive for organizations to comply with the law.

Commercial/Retail Organizations

The CGA proposes complaints-based investigative powers only, based on an oversight model closer to an ombudsman than a regulatory agency. Legislation should also allow the oversight agency to delegate powers and responsibilities to other jurisdictions and to assign complaints to existing processes. There should be time limits for investigations with safeguards against frivolous or repetitive complaints.

Enlogix supports ombudsman-like powers of investigation and audit. The CDMA reserves comment on enforcement measures until more details about an enforcement regime are publicly available.

Information Technology Associations

CATA, CAIP, and ITAC support complaints-based enforcement only. The Advanced Card Technology Association of Canada recommends broader powers, suggesting that site visits and audits by the oversight body are useful as remedial, rather than confrontational tools. CIPS says the oversight body needs the powers to compel organizations to produce evidence, and says it should be an offence to mislead or attempt to mislead the oversight body.

Individuals (including consultants, experts and academics)

Individuals generally seek proactive powers as per the powers currently available under the federal *Privacy Act*, including the powers of audit (two suggestions are that these powers should be equivalent to those of Revenue Canada or human rights commissioners).

There were two additional comments that these powers should either be used only to address the most serious complaints, much as the misleading advertising provisions of the *Competition Act* are handled, or where sectoral bodies have exhausted their processes or are likely to fail.

Highlights

Generally, all parties recognize the need for investigative powers when a complaint arises. Where detailed powers are recommended, they are generally in line with the existing powers of the federal Privacy Commissioner.

7. What powers are needed to address violations of the law and compensate individuals who have been harmed?

Consumer groups and privacy commissioners favour broad powers to address violations. Most parties support the power to publicize consumer complaints and non-compliance, without fear of liability, and some suggest this is one of the most important deterrent powers.

Consumer groups stress that fines should not simply become a cost of doing business. They should be set high enough so as to remove any business benefit of violating the law. Most business respondents feel that compensation should be left up to the courts with fines commensurate with actual damages. Specific comments are listed below.

Privacy Commissioners

The federal Privacy Commissioner supports a complaints model that encourages individuals to deal directly with organizations first. However, where there is evidence of non-compliance and harm to the individual, the Privacy Commissioner should have the ability to identify appropriate redress for the complainant. If an organization fails to implement recommendations made by the Privacy Commissioner, the Commissioner should have the power to publicize this fact. The Commissioner should also be able to refer matters to the Federal Court where compliance could be ordered, fines could be set and individuals could be compensated.

The Information and Privacy Commissioner of Alberta believes the federal Privacy Commissioner requires the powers to impose penalties and sanctions for wilful obstruction, determine issues of fact, find merit in complaints, grant remedies and award damages, limit liability in class action cases, and apportion liability between data users and processors.

The Information and Privacy Commissioner for BC proposes penalties and sanctions under criminal and civil processes, and the Information and Privacy Commissioner of Ontario proposes powers to require an organization to change or cease an information use or practice, and order the destruction of information. The federal Privacy Commissioner should also have the power to file an order with the Federal Court, making it a court order for enforcement purposes. In rare cases where an individual has truly suffered harm, the Privacy Commissioner should be able to award compensation.

The Commission d'accès suggests fines be established as per the Québec *Act*.

Consumer Groups (including organized labour)

Privacy Partners believes the oversight body needs the powers to publicize names, order audits, order third party investigations of policies and procedures, and set fines and award compensation.

CAC adds that penalties should be stiff and escalate with repetition. They should be

levied in reference to the offender's gross annual income and, where violation of privacy law is for personal gain, be related to the anticipated gain. PIAC supports this position, adding that every day an offence continues after notification should be considered a new offence. PIAC states that compensation should be provided for distress, annoyance and embarrassment. Designated offences should include failure to register, failure to report, and failure to submit a privacy impact assessment. Under the federal *Contraventions Act*, these should be considered strict liability offences in provincial courts.

PIAC adds that private citizens as well as the oversight agency, through the Attorney General, should have the right of criminal prosecution or for injunctive relief, both interim and final. The law should also set limitation periods on prosecutions in a way that will not hamper law enforcement ability. In addition, restitution orders should give prosecutors first call on court-imposed fines to recover costs, with a 50% award of any fine to the successful private prosecutor. Civil suits should be actionable by individuals as well as in class actions and State (substitute) actions. These actions should be pursuable in small claims court with damages awarded for distress, annoyance and embarrassment, a minimum recovery rule of $500, and an onus on the defendant to prove due diligence. Successful plaintiffs should be able to cover their legal and investigatory costs.

FIPA generally endorses the powers noted above and adds the oversight body should have the powers to approve or forbid indirect collection of personal information. FNACQ/OC endorses the powers noted within the Industry Canada discussion paper, and the BCCLA supports compensation as per precedents set in other administrative law contexts.

CUPE supports broad powers to enforce legislation, including the power to investigate, make binding orders, impose penalties, make remedial orders and order compensation.

Archivists/Historical/Library Associations

CLARA recommends a provision for fines in the legislation for wilful or deliberate violations of the law, while the OLA calls for legally binding enforcement and penalties in the same way as environmental violations are handled.

Telecommunications/Cable Sector

AT&T believes there should be consequences for failing to comply with fair information practices, but cautions that a public listing of non-compliant companies could have a significant negative impact on business. The CWTA believes the oversight body should only issue non-binding recommendations regarding complaints and concerns and, if action is not taken, the issue could be furthered resolved by the Federal Court. The CWTA says powers to address violations and compensate individuals are best left to the courts. The AT&T Companies and TELUS also believe enforcement and compensation powers should reside with the courts.

Stentor supports an oversight body's power to publicize findings, subject to an appeal mechanism prior to publication, but believes parties should be able to test issues of law or

jurisdiction before the Federal Court, and that provincial courts should resolve compensation issues.

Rogers supports powers to order specific performance, injunctive relief and limited fines to address violations of the law.

Financial Sector

The CBO believes that sectoral oversight bodies should have only the power of recommendation and the power to report publicly on how complaints were disposed of as an inducement to business to comply with the legislation. The CBO prefers a non-binding process and cautions that the principles of natural justice must apply to any binding decision-making powers given to a government oversight body.

CHLIA wants penalties and compensation dealt with in a manner consistent with the treatment of other aspects of market practice and consumer protection, while ACFC states that penalties and compensation are best left to the courts, which are familiar with the right to privacy as a civil right. Equifax, which is subject to provincial jurisdiction, notes that some, but not all provinces have legislation establishing the tort of invasion of privacy and many provincial courts have recognized this tort by common law jurisprudence.

ICC believes compensation for damages should only be awarded with proof of damage, and only to the extent that the company that breached the privacy law cannot first correct the damage. In many cases, the appropriate remedy would be for the company to correct the information and communicate corrected information to third parties where necessary.

CGA Ontario believes monetary compensation is best left to the courts, while the privacy legislation should provide for a statutory right of civil action similar to the United Kingdom *Data Protection Act, 1984*. Issues to resolve are whether business would have a defence to such an action based on taking reasonable measures under the *Act*, and what damage awards would be available if no actual damages could be proved.

Deloitte employees do not favour compensation for damages since this would only encourage complaints. Fines and publicizing of violations should suffice as deterrents.

Commercial/Retail Organizations

The CGA says there is no need to strengthen existing privacy laws with regard to violations and compensation. Enlogix proposes powers of mediation and recommendation, but does not support coercive powers.

Information Technology Associations

The Advanced Card Technology Association of Canada believes the federal Privacy Commissioner should be the ultimate oversight agency with powers to both impose penalties appropriate to the offence and award compensation to victims, commensurate with damages

suffered. CIPS supports powers to make binding orders through a tribunal to rectify non-compliance and to compensate individuals.

Individuals (including consultants, experts and academics)

Individuals who commented on this question have mixed views on the powers that should be available to address violations and compensate individuals. One wants limited sanctions available, but believes compensation should be handled separately. Another wants the judicial system to address violations and compensate. A third prefers a national model similar to Revenue Canada with powers to investigate and fine all business organizations, regardless of jurisdiction. A fourth states the powers should be as per existing privacy commissioners. There is also a comment that there should be mediation and arbitration powers to address small and honest errors without invoking an excessive level of intervention.

Of those who offered more specific comments on powers (four individuals), there is common agreement on the need for powers to make binding orders, award compensation and levy fines. One individual calls for powers to order cessation of organizational practices that violate the law and to force remedial corrective action with follow-up audits, as well as making offenders issue public apologies and publish details of violations. One individual suggests companies be prohibited from selling services for a defined period.

Where fines are mentioned, the view is that they should be in proportion to the size, nature and potential damages, and should be set high enough so that deliberate misuse of personal information not to become a cost of doing business. Another calls for fines payable to the wronged person of up to $100,000 and imputable to either the business or an individual employee.

Highlights

Consumer groups and privacy commissioners favour broad powers to address violations. Most parties support the power to publicize consumer complaints and non-compliance, without fear of liability, and several business and consumer groups as well as individuals suggest this is among the most important deterrent powers

8. Should there be powers to conduct independent research and proactive investigation/inspection of an organization's practices and to write reports?

There is general agreement that oversight bodies should have powers to conduct independent research *of a general nature*, since such research on new technologies and emerging privacy issues is of value to all parties.

There is, however, mixed support for proactive investigations of organizations. Most business submissions oppose proactive investigations. Among consumer groups, the CAC calls for investigative powers to act on suspicions and PIAC calls for the six-person threshold of the *Competition Act* (s.9) to be the basis to force a mandatory investigation by the federal Privacy Commissioner. The federal Privacy Commissioner suggests powers to conduct an issues-based audit where multiple complaints, investigation and mandatory mediation suggest systematically inadequate information practices. Other privacy commissioners support a similar position. Detailed comments are outlined below.

Privacy Commissioners

All privacy commissioners support powers to conduct independent research and proactive investigation and inspection.

Consumer Groups (including organized labour)

FIPA supports a complaints-driven model while all other organizations commenting on this issue generally support proactive powers, including powers to act on suspicions or rumours.

Privacy Partners notes, however, that only 15% of respondents to its survey feel the law should allow a company to be investigated at any time to make sure it is obeying the law, without the basis of a complaint.

Health Care Sector

CDA supports proactive powers of investigation, stating that privacy protection should be more than complaints-based.

Institutes

The U of O Centre believes privacy commissioners should be able to initiate investigations via privacy audits and technology impact assessments, and also carry out studies relating to privacy and emerging technologies.

Archivists/Historical/Library Associations

The OLA believes that powers to conduct independent research and investigation should be limited to actual violations of the law, as well as research and statistical reporting on data stripped of links to actual identity.

Telecommunications/Cable Sector

The AT&T Companies do not support proactive powers to inspect and investigate organizations, but do support independent research. Rogers and Microcell also claim proactive investigative powers are unnecessary and that investigation should be on a complaints-basis only. Microcell also recommends that the legislation should recognize the costs to organizations of investigations and inspections and allow those costs to be recoverable in the event an investigation is unfounded. Stentor companies do not oppose a requirement to report complaints received by companies, provided such reporting is done on a routine and purely statistical basis.

Financial Sector

The CBO, ICC and Equifax do not favour proactive investigation and inspection of organizations' privacy practices, stating that oversight should be complaints-driven. An oversight agency should be able to report, however, on systemic problems, monitor industries, examine new technologies and engage in public education.

CHLIA says only that the oversight model must be consistent with the treatment of other aspects of market practice and consumer protection.

Deloitte employees state only that an oversight body have monitoring powers. CGA Ontario supports audit powers and believes the oversight body should have the power to assess new technologies.

Commercial/Retail Organizations

The CGA supports complaints-based powers only. There were no other direct comments on this question .

Information Technology Associations

The Advanced Card Technology Association of Canada supports independent investigations such as site visits and audits. Other organizations are silent on this issue.

Individuals (including consultants, experts and academics)

All individuals who commented on this question support proactive powers of investigation.

Highlights

There is broad agreement that oversight bodies should have powers to conduct independent research *of a general nature*, since such research on new technologies and emerging privacy issues is of value to all parties. Most business submissions oppose proactive investigations, while privacy commissioners, consumer groups and individuals support broader powers to conduct investigations where multiple complaints, investigation and mandatory mediation suggest systematically inadequate information practices.

Distribution of Powers and Responsibilities

9. Should a central oversight authority be established to oversee the implementation of the new legislation, and if so, what powers should it have? Should this role be added to the responsibilities of the federal Privacy Commissioner or some other body?

The vast majority of respondents favour the use of the existing Office of the Privacy Commissioner as the oversight body.

There were a few alternate views put forward by specific industry groups. The cable television industry advocates continued use of their existing self-regulatory model under CRTC oversight. One respondent from the credit industry wants this industry to be exempt from legislation. Other regulated organizations subject to provincial legislation stressed their preference for continued oversight by provincial sectoral regulators.

10. Should a tribunal be established, or should a higher court be given the task of issuing binding decisions on complaints?

Overall, there is a slight preference for use of the Federal Court over tribunals. The use of the Federal Court may be even more favorable if processes, such as those suggested by PIAC (*see Question 7*), are put in place to make provincial courts (e.g. small claims court) more accessible for small actions. Specific views are noted below.

Privacy Commissioners

The federal Privacy Commissioner and the Commission d'accès support the use of the courts for binding decisions. The Commission d'accès notes this is currently the practice under the Québec *Act*.

The Information and Privacy Commissioner of Alberta prefers a tribunal to make final and binding decisions, stating that the courts are already overburdened. The Information and Privacy Commissioner for BC says that sectoral bodies such as the CDMA could make the initial decisions on privacy disputes with the federal Privacy Commissioner having final binding powers. Judicial review of Privacy Commissioner decisions should, however, be available on grounds of error in law, bias, absence of jurisdiction, and other administrative law issues. The Federal Court should hear such a review.

The Information and Privacy Commissioner of Ontario believes the federal Privacy Commissioner should have binding powers, but that a second, undescribed, level of appeal should be available in cases where compensation and restitution are awarded. The Ontario Commissioner says the ability to appeal decisions awarding compensation is appropriate.

Consumer Groups (including organized labour)

FIPA, PIAC and FNACQ/OC prefer the use of the Federal Court, with FNACQ/OC adding that the establishment of a tribunal such as the tribunal under the *Canadian Human Rights Act* is another option.

The CCC, CAC Ontario, BCCLA and CUPE support the use of a tribunal to issue binding decisions over use of the courts. Privacy Partners says, however, that the legislation should specifically state that nothing within the law prohibits individuals from using other remedies such as criminal charges and civil remedies.

Health Care Sector

CDA's view is that, with a sectoral self-regulation model, the federal Privacy Commissioner would be the tribunal of last resort.

Government (including the European Union)

The EU prefers courts and judicial review to tribunals.

Archivists/Historical/Library Associations

CLARA cites the Information and Privacy Commissioner of Ontario's role as a tribunal with the power to issue binding decisions as an efficient model, and states there is no need to establish an additional tribunal. The OLA advocates a tribunal be established as part of the Office of the Privacy Commissioner. This tribunal would resolve complaints at the highest level and impose legal penalties.

Telecommunications/Cable Sector

All respondents who commented on this issue prefer the use of the Federal Court.

Financial Sector

Under the CBO industry sector regulatory model, there would be no role for either a tribunal or the courts. The CLHIA has no clear position on this issue, while CGA Ontario and ACFC support the use of the courts.

Deloitte employees support the creation of a national tribunal to back up the use of sectoral oversight bodies. They claim the Canadian courts are overburdened while decisions on privacy should be made swiftly. Canada Trust and Equifax also support the creation of a special privacy tribunal. Canada Trust says the tribunal should be composed of industry, government and public representatives similar to the Canadian Payments Association. In Equifax's view, a national appeals tribunal would deal with complaints against federally regulated industries as well as appeals from decisions made by provincial tribunals.

Commercial/Retail Organizations

The CGA does not support the creation of a tribunal. Enlogix suggests an advisory committee of private sector specialists be appointed to advise a new private sector Privacy Commissioner (who would have no coercive powers).

Information Technology Associations

CATA and ITAC support use of the Federal Court. CAIP supports a tribunal structure within the Office of the Privacy Commissioner similar to existing tribunals such as the Copyright Board, although parties should have recourse to the Federal Court of Appeal for judicial review of any legal issues. CIPS supports a similar approach but says appeals should be between the organization and the Privacy Commissioner only, so as to prevent companies from using their greater financial resources in the appeal process to prevail over individuals.

Individuals (including consultants, experts and academics)

Individual opinion is equally divided between the use of the Federal Court for appeals or the creation of a tribunal for final oversight. One suggestion was for a tribunal, with the use of the Federal Court for judicial review, where appropriate.

Highlights

There is mixed support for the use of tribunals versus the Federal Court, and little in-depth discussion of the pros and cons of either approach. The majority of business groups prefer use of the Federal Court. Privacy commissioners and consumer groups are divided on the issue. Where a tribunal is preferred, it is generally on the basis of accessibility (e.g. the courts are clogged) and, in a few suggestions, to act as a national body that could play a role in harmonizing privacy protection across all jurisdictions (as in the Human Rights Tribunal or Competition Tribunal that were mentioned by a few parties as examples of such national bodies). Where a preference for the Federal Court exists, there is also mention in submissions from some consumer groups that the legislation should not prevent individual access to lower courts, such as provincial small claims courts, to claim damages and seek awards. In one consumer group submission, there is reference to a structured approach that would facilitate such legal actions

11. What use should be made of existing industry regulators or of industry-led self-regulatory mechanisms? How can such bodies be set up to satisfy business, consumer and government expectations?

All parties generally support the concept of organizations attempting to resolve disputes directly with individuals before involving the federal Privacy Commissioner.

There is also a strongly stated position in industry groups, notably telecommunications and the financial sector, that primary reliance be placed on industry self-regulation which could include self-regulatory oversight bodies, with the Privacy Commissioner as a final means to resolve disputes in cases where no satisfactory resolution can be arrived at between the parties, or when such a process is deemed likely to fail.

Within the financial sector and commercial/retail sector, many organizations also noted that they were currently subject to provincial sectoral oversight bodies, and were either subject to existing privacy protection provisions or expected such provisions to be added to sectoral oversight responsibilities.

Despite these various views, there is very little general support among respondents for the role of existing federal sector regulators such as the Canadian Radio-television and Telecommunications Commission (CRTC) or the Office of the Superintendent of Financial Institutions (OSFI). There is, rather, a strongly stated preference for ultimate oversight in the hands of the Privacy Commissioner, with assistance from federal sector regulators where required, and use of industry self-regulatory processes to the extent practical. The specific views of various parties are outlined below.

Privacy Commissioners

The federal Privacy Commissioner views his Office as the ultimate oversight agency, while working closely with existing business umbrella organizations, industry-specific associations and relevant government entities to address privacy issues through consultation, conciliation and negotiation and with the absolute minimum use of coercion and compulsion. There would be no formal role for sectoral regulators as oversight agencies.

This view is generally shared by provincial privacy commissioners who encourage sectoral bodies to take an active role in complaints resolution and development of sectoral codes.

Consumer Groups (including organized labour)

The CCC objects to the sharing of privacy oversight responsibilities with existing regulatory bodies and industry associations. CPI also believes a central body is preferable to multiple complaints-handling bodies serving specific industry groups or sectors. FIPA, FNACQ/OC, BCCLA,and CAC also oppose sectoral regulators.

CAC Ontario and Privacy Partners state their continuing support for industry-led oversight bodies, with Privacy Commissioner oversight. PIAC warns that sectoral regulators should only be used to either refer complainants to the federal Privacy Commissioner or oversee a concurrent regulatory regime. PIAC says the government should guard against companies invoking the "regulated conduct defence" for activities specifically authorized or sanctioned by sectoral regulators.

Health Care Sector

The CDA supports sectoral self-regulation with Privacy Commissioner oversight.

Archivists/Historical/Library Associations

The OLA, which also supports binding sectoral codes where all stakeholders agree, believes sectoral oversight bodies can play a role in oversight as the first level of appeal where resolution cannot be reached between the individual and the organization.

Telecommunications/Cable Sector

Rogers and the CCTA support the continuing role of the CRTC as an oversight body. Microcell also believes the CRTC can play a continuing useful role since it has the expertise and staff to supervise the companies it regulates. AT&T and Stentor, however, believe privacy oversight should migrate from the CRTC to the Privacy Commissioner.

With regard to industry self-regulatory bodies, The AT&T Companies support continued use of an existing telecommunications ombudsman who acts on behalf of a number of companies. The Ombudsman could refer complaints to the Privacy Commissioner who would have final authority. The CWTA says it would be willing to receive, review and attempt to resolve complaints on behalf of industry members, referring them to the Privacy Commissioner where complaints could not be mutually resolved. The cable industry notes that it has an existing and well-functioning self-regulatory organization, and promotes its continued use.

Financial Sector

Many financial sector respondents are subject to industry-specific oversight bodies (e.g. insurance regulators) and have developed self-regulatory processes as well. Consequently the vast majority of responses to this question call for the maximum use of industry self regulatory processes and industry sectoral regulators.

Canada Trust, however, believes trade associations and industry ombudsmen do not have the appropriate experience to oversee privacy protection and should have no formal, legislated role in privacy protection. CGA Ontario concurs, stating that the federal Privacy Commissioner has familiarity with the issues and existing legislation and privacy protection is the central part of the Office's mandate, not just one of many issues to be dealt with.

Commercial/Retail Organizations

CGA supports the maximum use of existing processes for complaints resolution. It is CGA's view that the Privacy Commissioner should be able to delegate responsibilities to other jurisdictions and processes.

Individuals (including consultants, experts and academics)

Nine individuals commented on this question. Two do not support any role for sectoral oversight bodies. One health care practitioner suggests self-regulatory bodies with publicly appointed members could serve the public interest in overseeing professional associations. Another individual directly opposes this view, saying that appropriate sanctions could only be imposed by the State. One individual calls for sectoral oversight bodies such as the CRTC and OSFI to have the broadest array of enforcement tools as possible, including powers to act on their own volition to resolve complaints, but that the Privacy Commissioner should have final oversight authority. Another calls for such sharing of privacy protection responsibilities as long as there is a consistent approach.

With regard to industry associations, there are two comments in support of their role in public education and industry education and as industry sector "watchdogs," but no support for a formal role under legislation.

Highlights

There is clear support for the federal Privacy Commissioner having ultimate oversight responsibilities. There is very little support for federal sector regulators, such as the Canadian Radio-television and Telecommunications Commission (CRTC) or the Office of the Superintendent of Financial Institutions (OSFI), having ultimate oversight responsibilities. There is, however, some support for industry self-regulatory organizations to assist in the complaints resolution process.

12. How should responsibilities for public education be assigned?

The most commonly stated position among all respondents is that public education should be a primary and mandated responsibility of the Privacy Commissioner. Several respondents add that adequate funding must be provided for this task. The Commission d'accès, which provides public education, notes a recent proposal by a committee of the Québec National Assembly calling for public education to be mandated to the Quebec Human Rights Commission. One respondent suggests the department of Canadian Heritage and provincial educational authorities play a role in education, and a second respondent suggests Consumer and Corporate Affairs ministries could play a role in distributing information.

There is also wide recognition that public education responsibilities must be shared with business and industry, trade unions, public interest and consumer groups, industry associations and others. Many private sector organizations note the existing obligations under the CSA Standard to be open about personal information policies and practices. The federal Privacy Commissioner calls for a requirement in the legislation that organizations should make specific information available about their management of personal information and their complaints resolution policies and practices without unreasonable cost or effort. Microcell suggests that the government follow the Information Highway Advisory Council recommendations to establish a working group of government agencies and consumer groups to increase public awareness and disseminate educational materials.

The Canadian Gas Association, however, takes an opposing view. CGA state that it sees no need for further public education, since education concerning private sector use of personal information should not exceed education about public sector use of personal information.

PIAC recommends that education funding be provided from registration of data users and from financial penalties for non-compliance. However, as noted under *Question 5*, there is little general support for registration schemes.

Since the nature and extent of private sector education is left entirely to the discretion of the private sector under the CSA Standard, the Information and Privacy Commissioner for BC calls for express statutory authority for public education to be shared by the Privacy Commissioner and private sector industries. However, the Information and Privacy Commissioner of Ontario suggests such a requirement within legislation would prove to be onerous and may, therefore, be ignored by business.

The role of the media was noted by several parties, and it is suggested in one submission that consumer groups can play an effective role in educating the public if they are funded to do so, since they have a high level of public credibility. It is also suggested that the Privacy Commissioner should enter into strategic partnerships with companies and associations to carry out this responsibility.

Highlights

Most respondents agree that public education should be the primary responsibility of the federal Privacy Commissioner. It should be listed as a duty under the proposed legislation, and adequate funds should be provided for it. Organizations should have an obligation to be open to the public about their own specific information use policies and practices, as specified within the CSA Standard.

13. Should the law require privacy impact assessments of new technologies? If so, when and by whom?

Most business organizations are opposed to privacy assessments imposed by law that might threaten technology innovation, create impossible hurdles for cash-strapped small companies and drive activities and jobs to other jurisdictions.

Most, but not all, consumer groups support mandatory legislated assessments, as do one or two individuals. Among privacy commissioners, however, only the Information and Privacy Commissioner for BC supports this position.

There are also differing views on who should perform privacy assessments. CIPS, for example, believes they should be conducted or overseen by the accountable individual within the organization. Consumer groups want a process that includes public input and public approvals. Specific positions are outlined below.

Privacy Commissioners

The federal Privacy Commissioner believes the Office should provide organizations with the tools necessary to conduct privacy impact assessments on any activity or proposed activity that may impact privacy. It is unclear whether such assessments would be mandatory.

The Information and Privacy Commissioner of Alberta supports industry-developed privacy impact assessments that are submitted to the federal Privacy Commissioner on a voluntary basis for advice and direction. The Alberta Commissioner raises a number of practical concerns about a mandatory legislated approach. The Commissioner states that, if they were a legislated requirement, it would likely create an unmanageable regime. Of particular concern is the fact that many advancements in technology take place outside of Canada's borders and, due to the transnational nature of many of these technologies, there may be no practical way to curtail their use until an impact assessment is performed and approved.

The Information and Privacy Commissioner of Ontario is a strong proponent of privacy impact assessments and believes the developer of the new technology is the best party to undertake the assessment, with a supporting role played by the Privacy Commissioner. The Commission d'accès adds that companies should complete assessments on their own initiative since they must already conform to privacy legislation.

The Information and Privacy Commissioner for BC, however, maintains that privacy impact assessments should be an essential legislated prerequisite to the promotion and use of new information technologies, new products and new services that collect, use, disclose, match, link, or store personal information. Assessments should be prepared by the organization responsible for the technology, product or service, should identify competing interests to the fullest possible extent and how a balance can be achieved, and should serve as a basis for consultation with the Privacy Commissioner.

Consumer Groups (including organized labour)

CAC Ontario supports a role for the federal Privacy Commissioner to conduct privacy impacts on new technologies as soon as they appear. Privacy Partners says such assessments should be mandatory and based on an assessment procedure developed through public consultation. FNACQ/OC says companies should be required under law to inform the Privacy Commissioner of their activities and to perform impact assessments before services are marketed or, preferably, at the design stage. Public consultation should follow each assessment.

PIAC adds that assessments should be mandatory for new information technologies and should be conducted by more than one party for comparative findings, with public review and comment. The Privacy Commissioner should be able to demand further assessments if required. The legislation should also clearly define the terms "information technologies" and "privacy impact assessment."

FIPA and BCCLA, however, do not support mandatory privacy impact assessments. BCCLA suggests they would be too onerous, and it is unclear what they would comprise and what status they might have. BCCLA suggests that inclusion of a principle of justification in the legislation would achieve the same value, since it would provide citizens with a means to challenge inappropriate information use practices. FIPA states that, when new technologies or services appear that affect privacy, the cost to maintain the previous standard of privacy should not be borne by the consumer.

Health Care Sector

The CDA states that basic principles should be developed by government that can form the basis for privacy impact assessments. CIHI considers itself to be the appropriate body to carry out such assessments in the health sector.

Institutes

The U of O Centre believes the Privacy Commissioner should have powers to initiate privacy investigations, including audits and privacy impact assessments.

Archivists/Historical/Library Associations

CLARA believes the Privacy Commissioner should be able to request that organizations conduct privacy impact assessments where data matching between organizations is planned. The OLA feels such assessments are impossible to do accurately, but suggests that new technologies be required to fit the spirit of the law.

Telecommunications/Cable Sector

All respondents are opposed to mandatory privacy impact assessments, stating it is incorrect to assume that all new technologies have the potential to erode privacy. They also assert that such assessments would be too costly and too difficult to implement and would have negative effects on the competitive position of Canadian businesses. The CCTA submits that

industry must be allowed to determine, on a voluntary basis, whether or not to perform a technology impact assessment, and that market reaction is the best determinant of whether or not privacy-enhancing technologies succeed or fail.

Financial Sector

Views on this issue are mixed. Some respondents oppose legal mandatory privacy impact assessments. Deloitte employees fear that "bureaucratizing" the process through legislation could be detrimental to technological growth and innovation, stating that the marketplace can be self-governing. ICC wonders how outcomes of such assessments would be used (e.g. would companies be prohibited from using technologies or would specifications on use be drawn up?). ICC also suggests that a set of standards could be drawn up by government for companies to measure the impacts of new technologies, as an aid to compliance. CHLIA adds that companies should assess the impact of new technologies at the development stage, without commenting on whether or not this should be a mandatory requirement.

CBA believes that, rather than legislating impact assessments, consumers should be informed of any risks in using new technologies. CGA Ontario, however, believes the Privacy Commissioner should have a mandate to assess new technologies, along with the power to audit organizational information use practices.

Commercial/Retail Organizations

CGA sees no need for mandatory privacy impact assessments.

Information Technology Associations

CATA, CAIP and ITAC believe mandatory privacy impact assessments would seriously impede innovation and the speed of getting new technology to market. CATA says they would be impossible hurdles for small, cash-strapped companies and would simply drive activities, and resulting jobs, into other jurisdictions. The Advanced Card Technology Association of Canada takes no firm position, but notes it collaborated on a privacy impact assessment with the Information and Privacy Commissioner of Ontario on smart, optical and advanced cards. CIPS, on the other hand, believes privacy assessments should be performed for any new program or business function, as well as new technologies, and should be conducted or overseen by the individual accountable within the organization for compliance with the legislation.

Individuals (including consultants, experts and academics)

Individuals generally support mandatory privacy impact assessments for new or privacy invasive technologies. One individual called for their use specifically for biometric and smart card technologies and said they should be ordered by the Privacy Commissioner, who could then decide to allow or disallow the use of a new technology, or refer the decision to a privacy tribunal. Two others said such assessments should be performed by the Privacy Commissioner. Two respondents, however, believe they should be performed by business organizations, with guidance from the Privacy Commissioner, with the results either submitted to the Privacy Commissioner for review or made publicly available upon request. One individual said the

Privacy Commissioner should develop the standard for privacy assessments, but did not define who should perform them. Another called for independent assessors and public hearings, much as with environmental impact assessments.

Highlights

There are differing views on the need for mandated privacy impact assessments. Business organizations are almost unanimously opposed to mandatory assessment which, in their view, might threaten technology innovation, create impossible hurdles for cash-strapped small companies and drive activities and jobs to other jurisdictions. Consumer groups have mixed views on mandatory assessments and who should perform them, while only one privacy commissioner supports legislated privacy assessments.

It may be possible to accommodate the interests of all parties in protecting personal information while not unduly impacting the advance of new technologies and services by encouraging, rather than requiring, privacy impact assessments under legislation. Such assessments could be performed by accountable individuals within organizations and could be a consideration in any subsequent investigation by the federal Privacy Commissioner

Cooperation

14. How should responsibilities for protecting personal information in the private sector be shared among the provincial, territorial and federal governments?

Most business organizations that responded to *Question 14* believe that harmonization is important, even critical, to the success of any legislated private sector privacy regime. Reasons provided on the importance of harmonization include the potential barriers to interprovincial trade; the need for an efficient, cost-effective legislative regime; the need for a level playing field for all sectors; the negative impacts of differing privacy standards on the development and delivery of electronic commerce; and the desire to avoid the growth of data havens.

Among Privacy Commissioners, there is general agreement on the need for harmonization to ensure equity across all regions of Canada, recognizing the existing division of powers.

Dr. Lorne Taylor, Alberta's Minister for Science, Research and Information Technology, also supported the need for harmonization, as well as recognizing the need to move forward on legislation, given European developments. The Minister cautioned, however, that the impacts of legislation on trading relationships with the U.S. would have to be considered.

With regard to the timing of federal private sector privacy legislation, Stentor states that federal sector legislation should not move forward until there is a clear commitment on the part of all provinces and territories to proceed as well. Other federally regulated telecommunications carriers, notably TELUS and the AT&T Companies, also caution against the competitive inequities that would be created by federal-only legislation. The CWTA, on the other hand, sees value in a federal government initiative that could clarify the application of legislation for other levels of government. Consumer groups also strongly support federal government leadership in this area.

Among financial institutions, insurance companies and securities regulators, as well as other organizations providing financial services, harmonization is generally considered an essential element; however, there is no specific comment from federally regulated financial institutions on whether or not the federal government should proceed first. Specific comments are outlined below.

Privacy Commissioners

Most privacy commissioners support a scope for federal legislation consistent with the existing division of constitutional powers under the *Constitution Act*, 1867. The Information and Privacy Commissioner of Alberta sees value in the possibility of national, all encompassing harmonized legislation to avoid a patchwork of inconsistent, possibly contradictory laws and regulations.

The Information and Privacy Commissioner of Ontario adds that there must be a process

for resolving situations where it is not clear which level of government has jurisdiction.

Consumer Groups (including organized labour)

FIPA supports sharing of powers between federal and provincial privacy commissioners as per the existing powers under the Constitution. BCCLA and CAC Ontario say the federal government should lead with legislation, followed by the provinces. BCOAPO concurs, adding that harmonized legislation is desirable but not essential, and a federal statute, broadly harmonious with Québec's *Act*, should be put forward for other provinces to follow. BCOAPO adds that the government could assert comprehensive jurisdiction over personal information protection through its exclusive jurisdiction over telecommunications (since the telecommunications system is used to electronically amass, store and manipulate information).

PIAC also calls on use of federal powers (trade and commerce power, criminal power and general residual power) to create a national harmonized regime, saying that reliance on provincial regulation will result in a patchwork of standards and enforcement methods. PIAC adds that the federal *Contraventions Act* could be used to accommodate enforcement of legislation through provincial authorities for efficiency reasons, including resolution of civil suits through small claims court.

Health Care Sector

The CNA notes that health care is a provincial responsibility and calls for a cooperative approach that blends federal coverage with separate provincial health acts.

Government (including the European Union)

Alberta states that harmonization is vital to future privacy legislation and urges the federal government to work with the provinces before drafting final legislation. Input from the Uniform Law Conference of Canada (ULCC) should also be encouraged prior to any federal legislation being proposed.

Archivists/Historical/Library Associations

CLARA advocates one national law or harmonized provincial laws within the private sector. The OLA says federal legislation should acknowledge but supercede existing sectoral and provincial statutes.

Telecommunications/Cable Sector

All respondents cite the need for national, harmonized privacy laws between federal and provincial jurisdictions so as not to disadvantage federally regulated industries and create an uneven patchwork of laws. TELUS stresses that legislation should not impose a greater burden on federally regulated sectors than on similar sectors within provincial jurisdiction. Microcell adds that legislation must not constrain companies operating in more than one part of Canada.

Rogers and the CWTA urge the federal government to work towards a system where

there is only one set of laws to prevent multiple and potentially conflicting obligations for business. The CWTA also believes that the federal government's initiative in this area could clarify the application of legislation for other levels of government.

Stentor, however, urges the federal government not to consider legislating until the provinces have committed to moving forward with equivalent harmonized legislation.

Financial Sector

All respondents cite the need for harmonization to a common standard. Canadian Central says harmonization across the country is important to provincially regulated organizations such as credit unions.

There are differing opinions, however, on how harmonization can be achieved. In Equifax's model, a national commission within the Office of the Privacy Commissioner would have ultimate oversight, both directly over federally regulated companies, and through an appeals process, over provincial privacy tribunals. The CBO model, which has a strong component of industry self-regulation, would limit the role of the Privacy Commissioner to referring complaints to sectoral organizations and monitoring the results, thus limiting the need for any federal-provincial harmonization of legislation.

CAFII and Canada Trust say the federal government should either replace, incorporate or defer to existing statutes, including federal and provincial financial institution and insurance statutes, that create conflict and duplication.

Commercial/Retail Organizations

The Sudbury and District Chamber of Commerce states that legislation needs to be flexible, consistent, applicable and enforceable across all jurisdictions. The CGA views harmonization as essential, stating that federal law should be confined to principles and include powers to delegate federal responsibility to the provinces to avoid duplication of process.

The CDMA proposes a model similar to the *National Health Act* with the federal government enunciating basic minimum standards, but leaving specific and detailed application to the provinces.

Information Technology Associations

All technology associations believe harmonization is important. The Advanced Card Technology Association of Canada recommends a scope of legislation to match the existing powers as per the *Constitution Act, 1868* and subsequent related laws.

Individuals (including consultants, experts and academics)

All individuals who commented on this question state that harmonization is important to ensure universal privacy rights in Canada and to ensure international recognition (e.g. to meet EU Directive requirements). Respondents, as a whole, believe each jurisdiction should legislate

within their own areas of responsibility.

One individual, however, calls for a new Canadian Privacy Board to oversee privacy implementation across Canada, but with authority only to investigate and comment.

Highlights

Most parties believe that harmonization is important, even critical, to the success of any legislated private sector privacy regime and to the marketplace, yet there are few specific recommendations on how to accomplish harmonization. There are conflicting views on whether the federal government should move unilaterally on legislation ahead of the provinces.

15. What forums, in addition to those discussed in the paper, would be useful in harmonizing the protection of personal information in all jurisdictions in Canada?

The Uniform Law Conference of Canada (ULCC) is mentioned by many respondents, reflecting broad awareness of the ULCC's current project to draft a model privacy law, and support for the role such a model law could play. There is also comment that the harmonization process can be advanced through such other forums as regular meetings of privacy commissioners, First Ministers' Conferences, annual conferences of Ministers of Justice and Attorneys General, Information Highway Ministers, Provincial Chief Information Officers, the Interprovincial Committee on Internal Trade, and the Minister of Health's Advisory Council on Health Info-structure.

There are calls for active representation from business associations, trade unions, consumer groups, the health sector, the archival community, sectoral regulators and other key interested parties in whatever additional forums are developed to discuss privacy legislation at both the federal and provincial levels.

Highlights

There is strong support for the work of the Uniform Law Conference of Canada (ULCC), which is drafting a model privacy law. A variety of other forums should also be used to advance harmonization of privacy protection across all jurisdictions. All forums should involve stakeholder input to the maximum extent.

General Conclusions

The above short summarization and analysis of submissions cannot begin to do justice to the many thoughtful and articulate comments put forward by all parties on the issue of private sector privacy legislation. Many comments relating to the general concept of privacy in the context of our technological society could not be included, although many were deserving of mention. Other points did not relate directly to the 15 questions could also not be reflected.

The consultation process elicited 90 responses, including many comprehensive and detailed documents that reflect, in general, the interest that all Canadians attach to the importance of privacy protection and achieving the right balancing of interests.

The extent of convergence in positions and the scope for compromise suggests that a balancing of interests, reflective of the legitimate interests of all parties, may be attainable with some further effort. There is clearly agreement on the CSA Standard as a good starting point for legislation, although some further effort will be required to find the appropriate degree of precision and to consider the additional obligations suggested by some parties, as well as to consider how best to accommodate the needs of journalists, credit reporting agencies, securities regulators, medical researchers and archivists and others within the framework of a privacy law.

There is clear support for the oversight role of the federal Privacy Commissioner, the need for some proactive powers of investigation and the need for public education. There is also active support for a complaints resolution process that starts with organizations, with strong encouragement for organizations to develop individual or sectoral codes of practice for guidance purposes.

It is also clear that virtually all parties encourage the development of a national framework of harmonized privacy laws that would apply across all jurisdictions to provide all Canadians with an equivalent measure of privacy protection, and to ensure a level playing field for business. Achieving this framework should be the most important objective in advancing privacy legislation.

APPENDIX 1:

INDEX
of Submissions to the Discussion Paper

1) Summaries of Submissions from Organizations

Advanced Card Technology Association of Canada (ACT)	1062
Alberta Minister Responsible for Science, Research And Information Technology, Dr. Lorne Taylor	1036
Association des archivistes du Québec	1077
Association of Canadian Financial Corporations (ACFC)	1028
AT&T Canada Enterprises	1041
AT&T Canada Companies: ACC TelEnterprises Inc.; AT&T Canada Long Distance Services Company; Call Net Enterprises Inc; fONOROLA Inc.; Westel Telecommunications Ltd.	1040
B.C. Civil Liberties Association (BCCLA)	1063
B.C. Freedom of Information & Privacy Association (FIPA)	1061
B.C. Public Interest Advocacy Centre (B.C. Old Age Pensioners' Association, the Consumers' Association of Canada BC Branch, the Council of Senior Citizens' Organizations, the Federated Anti-poverty Groups of B.C., the Senior Citizens' Association of B.C., the West End Seniors' Network, the B.C. Coalition for Information Access, End Legislated Poverty, and the Tenants' Rights Coalition) (BCOAPO)	1057
Bennett Gold Chartered Accountants, Robert Y. Gold	1026
Cable Television Standards Foundation	1044
Canada Trust	1059

Canada's Coalition for Public Information (CPI)	1021
Canadian Advanced Technology Association (CATA)	1030
Canadian Association of Financial Institutions in Insurance (CAFII)	1037
Canadian Association of Internet Providers (CAIP)	1085
Canadian Bankers Association	1092
Canadian Banking Ombudsman, Michael Lauber	1025
Canadian Cable Television Association (CCTA)	1083
Canadian Dental Association	1086
Canadian Direct Marketing Association (CDMA)	1016
Canadian Gas Association	1034
Canadian Historical Association (CHA)	1020
Canadian Information Processing Society (CIPS)	1084
Canadian Institute for Health Information (CIHI)	1071
Canadian Legislative and Regulatory Affairs Committee (CLARA) of the **Associations of Records Managers and Administrators Inc.** (ARMA International)	1055
Canadian Life and Health Insurance Association Inc.	1089
Canadian Newspaper Association	1047
Canadian Nurses Association	1046
Canadian Securities Administrators	1079
Canadian Union of Public Employees (CUPE)	1088
Canadian Wireless Telecommunications Association (CWTA)	1070
Certified General Accountants Association of Ontario (CGA Ontario)	1066
Commission d'accès à l'information du Québec	1095
Consumers' Association of Canada (Ontario)	1002

Consumers' Association of Canada	1060
Consumers Council of Canada	1093
Credit Union Central of Canada	1080
Deloitte and Touche (Yezdi Pavri, Robert Parker, Adel Melek, Brenda Eprile, Ian Tod, Karen Nemani, Nina Vivera)	1074
Dickson, Gary; Q.C., M.L.A. Calgary Buffalo, Legislative Assembly of Alberta	1067
Dun & Bradstreet Canada	1031
Enlogix Inc.	1049
Equifax Canada Inc	1023
European Union – Mr. John Mogg, Director General of DGXV Internal Market and Financial Services	1081
Faneuil ISG Inc.	1075
Fraser Institute, The	1015
Human Rights Research and Education Centre, University of Ottawa	1065
IMS Canada	1032
Information and Privacy Commissioner for British Columbia, David H. Flaherty	1018
Information and Privacy Commissioner of Alberta, Robert C. Clark	1078
Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian	1027
Information Technology Association of Canada (ITAC)	1043
Institut d'histoire de l'Amerique français	1069
Insurance Council of Canada/ Conseil d'assurances du Canada	1048
Metropolitan Halifax Chamber of Commerce	1017
Microcell Telecommunications Inc	1052

Ontario Library Association (OLA) 1058

Option Consommateurs; La Fédération nationale des associations de consommateurs du Québec (FNACQ) 1038

Privacy Commissioner of Canada, Bruce Phillips 1076

Privacy Partners Forum (Media Awareness Network; Public Interest Advocacy Centre; Canada's Coalition for Public Information; the Consumers' Association of Canada; Telecommunities Canada; la Fédération nationale des associations de consommateurs du Québec, and the Ottawa Public Library) 1073

Public Interest Advocacy Centre 1039

Rogers Communications Inc. 1042

Royal Canadian Mounted Police 1033

Stentor Telecom Policy Inc. (Bell Canada, BC TEL, Island Tel, MTS, MT&T, NB Tel, NewTel Communications, NorthwesTel, Québec Tél, SaskTel, BC TEL Mobility, Bell Mobility, Island Tel Mobility, MTS Mobility, MT&T Mobility, NB Tel Mobility, NewTel Mobility, Québec Tel Mobilité SaskTel Mobility, NorthwesTel Mobility) 1054

Sudbury and District Chamber of Commerce 1091

TELUS Corporation 1051

Vancouver Stock Exchange (VSE) 1045

Western Forum of Credit and Financial Executives 1022

2) Summaries of Submissions from Individuals

Bennett, Chris 1056

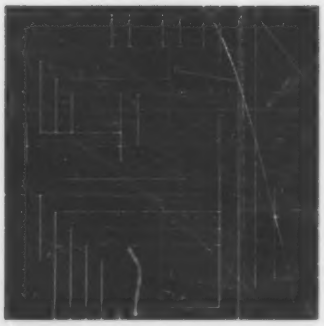
Bobier, Paul 1006

Brown, Glen R. 1013

Campbell, Terry; indie IDEAS 1035

Clement, Andrew; Associate Professor, University of Toronto	1064 (1068)
Fallis, Richard	1005
Fletcher, Tim; Hamilton-Wentworth Regional Police	1029
Harris, Don; HR Systems, The New York Times Company, and Chair, IHRIM Committee on Information Use and Protection	1053
Huband, Ken; Information Management Services	1014
Kuethe, Christopher	1009
Laninga, Ken	1007
Laughlan, Colin	1050
Litwyn, Jay	1008
Maurel, Richard-Philippe	1010
McNaughton, D.M.	1019
Meek, Chet	1004
Newcombe, Howard B.	1003
Siebert, Andreas	1011
Soskolne, Dr. Colin	1012
Speers, Richard D.	1072
Williams, Colin J.	1024

Gouvernement du Canada | Government of Canada



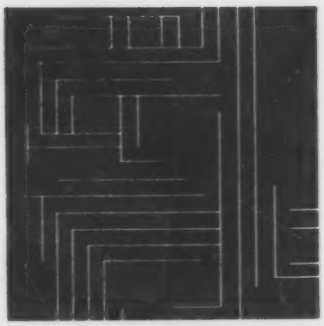
LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

POUR UNE ÉCONOMIE ET UNE SOCIÉTÉ DE L'INFORMATION AU CANADA

Rapport sommaire
des réponses au
document de travail

Juillet 1998

Canada



LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

POUR UNE ÉCONOMIE ET UNE SOCIÉTÉ DE L'INFORMATION AU CANADA

Rapport sommaire
des réponses au
document de travail

Juillet 1998

Le présent document est également diffusé en version électronique sur le Web à l'adresse **http://strategis.ic.gc.ca/vieprivee**

Il est aussi offert sur demande dans une présentation adaptée à des besoins particuliers. Communiquer avec les personnes dont les coordonnées figurent ci-dessous.

Pour obtenir des exemplaires du présent document, s'adresser à :

Diane Breau
Groupe de travail sur le commerce électronique
Industrie Canada
300, rue Slater, 20e étage
Ottawa (Ontario) K1A 0C8

Téléphone : (613) 991-4029
Télécopieur : (613) 941-0178
Courrier électronique : breau.diane@ic.gc.ca

Pour communiquer avec Murray Long :

Murray Long Communications and Policy Consulting
640, avenue LaVérendrye
Gloucester (Ontario) K1J 7C4

Téléphone : (613) 747-9651
Télécopieur : (613) 747-6261
Courrier électronique : murray.long@sympatico.ca

Nota – Aux fins du présent document, la forme masculine désigne, s'il y a lieu, aussi bien les femmes que les hommes.

© Sa Majesté la Reine du chef du Canada (Industrie Canada) 1998
N° de catalogue C2-355/1998
ISBN 0-662-63706-2
52007B

Also available in English under the title: *The Protection of Personal Information: Building Canada's Information Economy and Society – Summary Report of the Responses to the Discussion Paper*

Table des matières

Introduction	1
Résumé	5
Analyse détaillée des mémoires	13
Obligations	13
Pouvoirs	49
Répartition des attributions	67
Coopération	82
Conclusions générales	88
Annexe 1. Liste des mémoires reçus en réponse au document de travail	89

I Introduction

Le 27 janvier 1998, Industrie Canada et le ministère de la Justice ont publié un document de travail intitulé *La protection des renseignements personnels – Pour une économie et une société de l'information au Canada*. À la date limite pour la présentation des mémoires, soit le 27 mars suivant, les responsables en avaient reçu au total 83, tant des documents détaillés émanant d'associations industrielles que des messages électroniques d'une seule page transmis par des particuliers. Ils ont reçu après la date limite sept autres mémoires, qui sont compris dans la présente analyse.

Sur les 90 mémoires reçus, 22 provenaient de particuliers, dont trois d'universitaires, quatre d'experts de la protection de la vie privée ou de consultants et un d'un député de l'assemblée législative de l'Alberta.

Parmi les organisations, le Commissariat à la protection de la vie privée du Canada et les commissaires à l'information et à la protection de la vie privée de l'Alberta, de la Colombie-Britannique, de l'Ontario et du Québec ont présenté un mémoire en réponse au document de travail. Les responsables ont reçu 10 mémoires de groupes de défense des consommateurs, un d'une organisation syndicale (Syndicat canadien de la fonction publique), quatre d'organismes du secteur des soins de santé, cinq d'organisations représentant des archivistes, des historiens, des bibliothécaires et des gestionnaires de dossiers ainsi que un d'un organisme d'application de la loi (Gendarmerie royale du Canada). Le gouvernement de l'Alberta a présenté un mémoire, tout comme l'Union européenne.

Quant aux groupes du milieu des affaires, les responsables ont reçu cinq mémoires d'associations industrielles dont les membres s'intéressent aux questions de la technologie de l'information et du commerce électronique, soit l'Association canadienne de la technologie des cartes (ACT Canada), l'Association canadienne des fournisseurs Internet (ACFI), l'Association canadienne de technologie de pointe (ACTP), l'Association canadienne de l'informatique (ACI) et l'Association canadienne de la technologie de l'information (ACTI). Ils ont aussi reçu sept mémoires d'organisations du milieu des affaires représentant à la fois les intérêts du commerce de détail classique et ceux du marketing direct. Enfin, ils ont reçu un mémoire d'une organisation représentant les intérêts des médias, en l'occurrence l'Association canadienne des journaux (ACJ) ainsi que 6 mémoires faisant valoir le point de vue des entreprises de télécommunications assujetties à la réglementation fédérale par l'entremise du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), 3 mémoires de l'industrie de la câblodistribution, qui est aussi assujettie à la réglementation du CRTC et 2 d'organisations représentant des institutions financières sous réglementation fédérale ainsi que 14 mémoires représentant à la fois des sociétés sous réglementation fédérale ou provinciale œuvrant dans le secteur des finances, des assurances, des valeurs mobilières et de l'évaluation du crédit ainsi que des associations professionnelles faisant partie de ce secteur au sens large.

Au moment d'analyser les mémoires, nous avons dû examiner un grand nombre de suggestions réfléchies et originales sur la façon d'élaborer, de mettre en œuvre et d'appliquer une loi sur la protection des renseignements personnels. Certains points ont fait l'objet d'un consensus. Par ailleurs, comme on pouvait s'y attendre, certaines suggestions sont diamétralement opposées et il s'agit probablement en pareil cas des deux extrêmes de la gamme d'opinions sur une question donnée. Toutefois, dans la plupart des cas, nous avons reçu des suggestions qui présentent un certain degré de flexibilité quant à la manière d'aborder diverses questions.

Sur certaines questions, il y a entre les secteurs et au sein de chacun d'entre eux autant de divergence d'opinions que de convergence, qu'il s'agisse des commissaires, des groupes de défense des consommateurs, des particuliers ou des organisations du milieu des affaires.

De plus, certains mémoires provenant du milieu des affaires reflètent le point de vue de groupes de professionnels qui travaillent dans un secteur de l'industrie. Nous avons constaté que la manière d'aborder les questions dans ces mémoires est très différente du point de vue des organisations du même secteur. Il est à noter que ces organisations peuvent être assujetties à différents régimes de surveillance – fédéral, provincial, ou les deux – ou n'être assujetties à aucun d'entre eux.

Enfin, les répondants ont proposé une grande variété de modèles pour assurer la protection des renseignements personnels sur le marché commercial, d'où la difficulté d'organiser et de comparer de manière utile les réponses reçues. Pour le lecteur, il sera toutefois intéressant de savoir dans quelle mesure les opinions convergent ou si elles reflètent, par exemple, le point de vue du milieu des affaires, celui des consommateurs ou celui des commissaires.

Pour faciliter l'analyse des divers points de vue exprimés, nous avons classé les répondants en différentes catégories : les commissaires; les groupes de défense des consommateurs (y compris les mouvements syndicaux); le secteur des soins de santé; un organisme d'application de la loi; les administrations publiques, y compris l'Union européenne; les instituts; les associations d'archivistes, d'historiens et de bibliothécaires; le secteur des télécommunications et de la câblodistribution; le secteur financier au sens large; les organisations commerciales, y compris les commerces de détail; les associations du secteur de la technologie de l'information; ainsi que les particuliers, y compris les consultants, les experts et les universitaires. Certains répondants estimeront peut-être que cette catégorisation arbitraire ne permet pas de refléter équitablement ou exactement leur point de vue dans le cadre de l'ensemble des intérêts représentés et nous les prions de nous en excuser si tel est le cas.

Certains répondants ont formulé des commentaires éclairés sur la nécessité d'adopter une loi sur la protection des renseignements personnels ou analysé en détail la façon dont leur groupe industriel protège actuellement les renseignements personnels. Nous avons choisi la plupart du temps de ne pas faire état de ces commentaires généraux dans les résumés et de mettre plutôt

l'accent sur les réponses précises aux 15 questions posées dans le document de travail. C'est pourquoi le mémoire présenté par certains particuliers est aussi long ou presque aussi long que celui du mémoire de grandes organisations.

Les lecteurs qui désirent obtenir plus de détails ou des précisions sur les points de vue exprimés sont invités à lire les résumés. Si cela ne suffit pas, ils peuvent communiquer avec le Groupe de travail sur le commerce électronique pour obtenir une copie des mémoires qui les intéressent. Bon nombre des mémoires renferment beaucoup plus de renseignements que le présent document sur les questions et les préoccupations en matière de protection des renseignements personnels et sur les initiatives du secteur privé dans le domaine.

Murray Long

Suzanne Andrew

Résumé

Le document de travail d'Industrie Canada et du ministère de la Justice du Canada intitulé *La protection des renseignements personnels – Pour une économie et une société de l'information au Canada*, a donné lieu à la présentation de 90 mémoires, tant des documents détaillés émanant d'associations industrielles que des messages électroniques d'une seule page. Parmi les mémoires figuraient deux sondages. Le premier a été mené par la Chambre de commerce métropolitaine de Halifax auprès des 1 400 entreprises qui en sont membres, tandis que le second a été réalisé sur Internet par le Forum sur la vie privée, coalition formée de groupes de défense des consommateurs, du Réseau Éducation-Médias et de la Bibliothèque publique d'Ottawa. Le sondage de la Chambre de commerce a permis de recueillir une vaste gamme d'opinions, variant entre l'appui et une vive opposition à l'élaboration d'une loi simple. Quatre vingts pour cent des 51 répondants ont indiqué que l'adoption d'une loi aurait une incidence sur leurs activités. Pour sa part, le Forum sur la vie privée a reçu 270 réponses, toutes très favorables à l'adoption d'une loi sur la protection des renseignements personnels.

Les mémoires reçus de toutes les parties en réponse au document de travail d'Industrie et du Justice Canada ont été résumés et analysés en fonction des 15 questions posées. Il est à noter que certains commentaires dépassaient la portée du document de travail. Certains mémoires, provenant tant du milieu des affaires que d'autres groupes, ne portaient que sur une partie des 15 questions et renfermaient des commentaires uniquement sur les points qui intéressaient le plus les répondants.

Pour faciliter l'analyse, nous avons classé les répondants en différentes catégories : les commissaires; les groupes de défense des consommateurs, y compris les mouvements syndicaux; le secteur des soins de santé; un organisme d'application de la loi; les administrations publiques, y compris l'Union européenne; les instituts; les associations d'archivistes, d'historiens et de bibliothécaires; le secteur des télécommunications et de la câblodistribution; le secteur financier au sens large; les organisations commerciales, y compris les commerces de détail; les associations du secteur de la technologie de l'information; ainsi que les particuliers, y compris les consultants, les experts et les universitaires.

Les réponses à un certain nombre de questions ont révélé un appui clair à l'égard d'une orientation particulière. Par exemple, le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation (norme de la CSA) est considéré presque unanimement comme étant un bon point de départ pour la rédaction de la loi, bien que les commissaires, les groupes de défense des consommateurs et certaines organisations du milieu des affaires estiment nécessaire d'ajouter d'autres obligations ou de faire en sorte que la loi soit plus précise que la norme de la CSA.

Il y a aussi un accord presque unanime sur la nécessité d'harmoniser les lois fédérales et provinciales sur la protection des renseignements personnels, en vue d'assurer une application uniforme, d'empêcher l'érection d'obstacles au commerce interprovincial et de contrer la croissance des refuges de données. En outre, la plupart des répondants estiment que la Conférence sur l'uniformisation des lois au Canada (CULC) constitue la meilleure instance pour assurer l'harmonisation des lois fédérales et provinciales sur la protection des renseignements personnels.

La vaste majorité des répondants souhaitent que le Commissariat à la protection de la vie privée du Canada serve d'organisme de surveillance. De même, un très grand nombre estiment qu'il s'agit de l'organisme le mieux placé pour assurer l'éducation du public dans le domaine.

Par ailleurs, de nombreux répondants croient que les codes sectoriels jouent un rôle utile dans la protection des renseignements personnels, mais le remplacement de la loi par ces codes ne reçoit guère d'appui. En outre, peu de répondants sont favorables à des obligations initiales, comme l'enregistrement des codes de protection de la vie privée auprès d'un registraire accrédité ou d'un organisme de surveillance.

On observe des opinions très variées sur plusieurs autres questions. Mentionnons notamment les questions de la divulgation de renseignements sans consentement et des exclusions du champ d'application de la loi, ainsi que celles des pouvoirs d'application de la loi, de la création d'un tribunal ou du recours à la Cour fédérale, du rôle des organismes de réglementation de l'industrie et de la nécessité d'évaluer les incidences qu'ont les nouvelles technologies sur la protection des renseignements personnels.

Quant à savoir si la norme de la CSA est suffisamment précise dans l'énoncé des obligations, les commissaires, les groupes de défense des consommateurs et les particuliers sont généralement tous d'avis qu'il faut modifier la norme de la CSA pour la rendre plus précise et y ajouter de nouvelles obligations, par exemple, exiger la justification des fins visées par la collecte des renseignements. Certaines organisations du milieu des affaires estiment aussi que la loi doit être plus précise pour permettre la collecte et l'utilisation de certains types de renseignements et établir des règles claires et prévisibles dans le cadre desquelles les entreprises peuvent exercer leurs activités.

Comme les mémoires des groupes de défense des consommateurs et des groupes du milieu des affaires révèlent que ces deux parties souhaitent que la norme de la CSA soit plus précise, on pourrait réviser cette dernière dans le but de donner suite à leur préoccupation. Certaines suggestions détaillées formulées dans les mémoires, destinées à assurer une certitude accrue parmi les entreprises concernant les modes d'utilisation des renseignements, pourraient nuire à la souplesse de la norme actuelle de la CSA. Or, la majorité des entreprises souhaitent le maintien de cet aspect.

La majorité des entreprises estiment qu'il ne faut pas modifier de quelque façon que ce soit la norme de la CSA, car celle-ci leur offre la souplesse nécessaire pour exercer leurs activités. Les entreprises soutiennent qu'elles ont besoin d'un cadre législatif peu contraignant, qui n'entrave pas indûment les activités commerciales. On pourrait en arriver à un juste équilibre en examinant conjointement les questions de la précision, des obligations et de la nature des pouvoirs de surveillance proposés par les différentes parties. À cet égard, plus la loi sera imprécise, plus il faudra accroître les pouvoirs de surveillance, et vice versa, pour que les droits à la protection des renseignements personnels soient protégés de façon adéquate et qu'un juste équilibre soit maintenu entre les divers intérêts.

La question de la divulgation de renseignements sans consentement et des exclusions du champ d'application de la loi offre une autre occasion d'établir un équilibre qui permettrait de répondre aux besoins de toutes les parties. Les archivistes et les médias souhaitent que les renseignements de nature historique et le matériel journalistique soient exclus du champ d'application de la loi. Dans ce cas, en décidant plutôt d'inclure ces activités dans les types de renseignements qui pourraient être utilisés et divulgués sans consentement, on pourrait à la fois satisfaire les intéressés et assurer le respect des autres principes de protection de la vie privée, comme la responsabilité, la définition des fins visées par la collecte des renseignements et les mesures de sécurité.

En ce qui concerne les enquêtes sur les plaintes, toutes les parties conviennent généralement que les consommateurs doivent d'abord s'adresser directement à l'organisation visée, puis à un organisme de surveillance s'il n'a pas été possible de régler la plainte. De nombreux répondants estiment que le commissaire à la protection de la vie privée du Canada doit assumer les responsabilités ultimes en matière de surveillance. Ils ne sont guère nombreux à préconiser que ces responsabilités soient assumées par des organismes sectoriels de réglementation du niveau fédéral, comme le CRTC ou le Bureau du surintendant des institutions financières (BSIF). Certains, toutefois, souhaitent que les organismes d'autoréglementation de l'industrie participent au processus de règlement des plaintes.

En ce qui concerne les pouvoirs nécessaires pour l'application de la loi, une forte proportion de répondants, qui ne sont pas unanimes parmi les groupes du milieu des affaires, sont favorables à des pouvoirs de surveillance préventive, qui comprendraient celui de mener des enquêtes indépendantes sur les plaintes. Les opinions varient toutefois grandement quant à la façon de dédommager ceux qui ont subi un préjudice. Les répondants ne s'entendent pas non plus quant à la nécessité de rendre obligatoire l'évaluation des incidences qu'ont les nouvelles technologies sur la protection des renseignements personnels, ni quant à la façon dont doivent être menées les évaluations.

I. Faits saillants

Les faits saillants ci-dessous s'inspirent de la section Analyse détaillée du présent rapport, où ils sont présentés plus en détail. Ils représentent la diversité des opinions exprimées par les répondants. Dans certains cas, les auteurs ont formulé quelques suggestions en vue de répondre aux préoccupations de toutes les parties.

(Nota : Les conclusions sont numérotées et organisées en fonction des 15 questions posées dans le document de travail.)

1. Les répondants reconnaissent généralement que la loi doit s'inspirer de la norme de la CSA. Toutefois, au moment de la rédaction de la loi, il faudra tenir compte des commentaires formulés par les diverses parties, y compris les commissaires à l'information et à la protection de la vie privée, les groupes de défense des consommateurs, les organisations du milieu des affaires, les groupes d'intérêt et les particuliers, relativement à la nécessité d'une précision accrue et d'obligations supplémentaires.

2. Diverses organisations du milieu des affaires et d'autres parties sont d'avis que la divulgation sans consentement de certaines catégories de renseignements doit être possible. D'autres parties, y compris les commissaires ainsi que les groupes de défense des consommateurs, souhaitent que l'on dresse une liste extrêmement limitée et très précise des catégories de renseignements et des situations pouvant donner lieu à la divulgation sans consentement. Certaines parties ont signalé qu'aucune liste de cette nature ne peut être exhaustive. À la lumière des différents points de vue exprimés, la meilleure approche serait peut-être d'inclure une liste détaillée d'exemples de divulgation sans consentement prévus dans la loi, et d'indiquer dans quelles circonstances elle serait normalement permise. On doit également prendre en considération la suggestion formulée par quelques parties, selon laquelle les organisations doivent être tenues de documenter et de justifier la divulgation de renseignements en pareil cas.

3. L'appui exprimé à l'égard de la reconnaissance de codes sectoriels ayant force exécutoire est limité. En général, les répondants ont indiqué qu'aucune disposition de la loi ne doit permettre que les codes sectoriels remplacent la loi, ni qu'ils aient une reconnaissance légale, y compris une valeur interprétative. Un mémoire provenant du milieu des affaires, en particulier, a soulevé la question de la valeur interprétative de ces codes (c'est-à-dire que les tribunaux, au moment de déterminer une sanction ou une indemnité, doivent prendre en considération la manière dont l'organisation a interprété la loi en fonction de son code sectoriel). Un mémoire d'un groupe de défense des consommateurs souligne cependant que la nécessité d'empêcher les organisations d'utiliser la « défense impénétrable » selon laquelle elles ont appliqué de bonne foi la norme de la CSA

constitue une raison fondamentale pour laquelle la loi doit être plus précise. Étant donné ces opinions incompatibles, il serait peut-être préférable de laisser aux tribunaux le soin de trancher la question de la valeur interprétative, et ce, sans directives dans la loi.

4. Les mémoires indiquent que la définition de la notion de « personne » figurant dans la loi doit inclure uniquement les personnes physiques pour éviter que les organisations jouissent des droits à la protection des renseignements personnels dévolus aux particuliers. En outre, les rédacteurs de la loi doivent déterminer s'il est nécessaire d'établir une distinction entre les renseignements du domaine public à vaste diffusion et les renseignements publics qui ne sont pas destinés à une vaste distribution ou utilisation. En ce qui concerne les catégories d'utilisateurs de données, les rédacteurs doivent déterminer s'il convient d'exclure ces utilisateurs de tout le champ d'application de la loi ou de les exclure de dispositions particulières (par exemple, de l'obligation d'obtenir le consentement avant la collecte, l'utilisation ou la divulgation de renseignements).

5. Ceux qui appuient la mise en place d'un mécanisme d'enregistrement semblent préconiser la création d'un dépôt central de codes et d'un répertoire indiquant les coordonnées des personnes-ressources. Étant donné que les commissaires n'appuient pas ce concept et qu'il est possible, en vertu de la loi, d'obtenir les renseignements en s'adressant directement aux organisations, la mise en place d'un mécanisme d'enregistrement ne semble pas nécessaire

6. En général, toutes les parties reconnaissent qu'une entité doit avoir les pouvoirs requis pour faire enquête en cas de plainte. Lorsqu'elles recommandent des pouvoirs détaillés, ils sont généralement en harmonie avec les pouvoirs actuels du commissaire à la protection de la vie privée du Canada.

7. Les groupes de défense des consommateurs et les commissaires sont favorables à la création de vastes pouvoirs pour sanctionner les infractions. La plupart des parties préconisent le pouvoir de rendre publics les plaintes des consommateurs et les cas de non-conformité, sans crainte de responsabilité, et plusieurs groupes du milieu des affaires et de défense des consommateurs ainsi que des particuliers estiment que ces pouvoirs sont au nombre des plus importants pouvoirs de dissuasion.

8. La plupart des répondants sont d'avis que les organismes de surveillance doivent être habilités à mener des recherches indépendantes *de nature générale*, étant donné que les recherches sur les nouvelles technologies et les questions de protection des renseignements personnels qu'elles posent présentent un intérêt pour toutes les parties. La plupart des groupes du milieu des affaires s'opposent à la tenue d'enquêtes préventives, tandis que les commissaires, les groupes de défense des consommateurs et les particuliers sont favorables à la création de vastes pouvoirs pour faire enquête, par exemple, dans le cas où le nombre de plaintes, d'enquêtes et de médiations obligatoires laisse supposer

qu'une organisation a des pratiques en matière d'information systématiquement inadéquates.

9. La vaste majorité des répondants préconisent que le Commissariat à la protection de la vie privée du Canada agisse à titre d'organisme de surveillance.

10. Les avis sont partagés quant au recours aux tribunaux administratifs ou à la Cour fédérale et, en général, les mémoires ne traitent pas à fond des avantages et des désavantages de ces deux approches. La majorité des groupes du milieu des affaires privilégient le recours à la Cour fédérale. Les commissaires et les groupes de défense des consommateurs sont partagés sur la question. Ceux qui privilégient le recours à un tribunal le font généralement pour une question d'accessibilité (les cours sont engorgées); quelques-uns ont proposé que le tribunal agisse à titre d'organisme national qui contribuerait à harmoniser la protection des renseignements personnels dans l'ensemble des provinces et des territoires (d'après certaines parties, le Tribunal des droits de la personne ou le Tribunal de la concurrence pourrait être cet organisme national). Pour ce qui est du recours à la Cour fédérale, certains groupes de défense des consommateurs indiquent que la loi ne doit pas empêcher les particuliers d'avoir accès à des cours inférieures, comme les cours des petites créances des provinces, pour réclamer des dommages-intérêts. Un groupe de défense des consommateurs propose de mettre en place une approche structurée pour faciliter les poursuites en justice.

11. Les répondants estiment généralement que le commissaire à la protection de la vie privée du Canada doit assumer la responsabilité ultime en matière de surveillance. L'attribution de la responsabilité de surveillance ultime aux organismes sectoriels de réglementation sectoriels fédéraux comme le CRTC ou le BSIF ne recueille guère d'appui. Toutefois, certains souhaitent que les organismes d'autoréglementation de l'industrie participent au processus de règlement des plaintes.

12. Selon l'opinion exprimée par la plupart des répondants, l'éducation du public devrait être la principale responsabilité du commissaire à la protection de la vie privée du Canada. Il faudrait préciser dans la loi qu'il s'agit d'une fonction incombant au commissaire et faudrait prévoir les fonds nécessaires pour lui permettre de s'en acquitter. Les organisations doivent avoir l'obligation de faire montre de transparence concernant leurs politiques et pratiques en matière d'utilisation de l'information, comme il est précisé dans la norme de la CSA.

13. Les opinions divergent quant à la nécessité de prévoir dans la loi l'évaluation des incidences qu'ont les nouvelles technologies sur la protection des renseignements personnels. Les organisations du milieu des affaires s'opposent presque à ce que les évaluations soient rendues obligatoires, ce qui pourrait à leur avis nuire à l'innovation technologique, créer des obstacles insurmontables pour les petites entreprises disposant

de peu de liquidités et détourner ailleurs les activités et les emplois. Les groupes de défense des consommateurs ont exprimé des opinions partagées concernant les évaluations obligatoires et sur les intervenants qui devraient y procéder. Un seul commissaire souhaite que les évaluations soient prévues par la loi.

Il pourrait être possible de répondre aux intérêts de toutes les parties en protégeant les renseignements personnels, sans avoir une incidence indue sur l'évolution des nouvelles technologies et des nouveaux services, en précisant dans la loi qu'on encourage, plutôt qu'on exige, la réalisation d'évaluations. Les personnes responsables au sein des organisations pourraient procéder aux évaluations, qui pourraient par la suite être examinées dans le cadre de toute enquête ultérieure menée par le commissaire à la protection de la vie privée du Canada.

14. La plupart des parties estiment que l'harmonisation est importante, voire essentielle, pour la réussite de tout régime de protection des renseignements personnels dans le secteur privé prévu par la loi et pour le marché. Pourtant, elles donnent peu d'instructions précises sur la façon d'assurer l'harmonisation. Les opinions sont partagées quant à savoir si le gouvernement fédéral devrait agir unilatéralement et adopter une loi sans attendre que les provinces fassent de même.

15. De nombreux répondants se réjouissent du travail accompli par la CULC, qui rédige actuellement un avant-projet de loi-type sur la protection des renseignements personnels. Toutefois, on doit aussi faire appel à d'autres instances pour faire progresser l'harmonisation de la protection des renseignements personnels dans tous les secteurs de compétence. Les instances doivent faire intervenir le plus possible les parties intéressées.

Analyse détaillée des mémoires

L'analyse des recommandations et des commentaires formulés à l'intention d'Industrie Canada dans les divers mémoires reçus reprend l'ordre des questions de la partie 3 (*La parole est à vous*) du document de travail. Elle fait état de toute une gamme de suggestions précises et détaillées concernant l'adoption d'une loi sur la protection des renseignements personnels dans le secteur privé, mais elle n'englobe pas toutes les suggestions formulées.

Obligations

1. La norme de la CSA doit-elle servir de point départ à la rédaction de la loi? Est-elle assez précise dans l'énoncé des obligations ou faut-il apporter des éclaircissements? Y a-t-il d'autres obligations que celles figurant dans la norme de la CSA et qui devraient figurer dans la loi?

La *question n° 1* est celle qui a suscité le plus grand nombre de commentaires. Cela tient à la grande divergence des opinions exprimées concernant l'adoption d'une loi sur la protection des renseignements personnels dans le secteur privé et la façon de l'aborder.

Tous les commissaires à l'information et à la protection de la vie privée, les groupes de défense des consommateurs, les instituts, les universitaires, les experts, les consultants et les autres personnes qui se sont exprimées sont très favorables à l'adoption d'une loi. Les mémoires de l'Union européenne et du gouvernement de l'Alberta préconisent également l'adoption d'une loi fédérale sur la protection des renseignements personnels dans le secteur privé, mais le gouvernement de l'Alberta insiste sur la nécessité de mener des consultations soutenues auprès des provinces avant de promulguer une loi fédérale dans le domaine.

En revanche, les auteurs de mémoires du secteur privé n'estiment pas tous qu'une loi sur la protection des renseignements personnels soit nécessaire. Ainsi, l'Association canadienne du gaz (ACG) et l'entreprise de marketing direct Faneuil ISG Inc. estiment qu'une protection additionnelle des renseignements personnels n'est pas nécessaire pour l'instant. Selon Equifax Canada (Equifax), il ne faudrait pas légiférer sans avoir au préalable prouvé de façon empirique que les codes volontaires ne donnent pas des résultats adéquats. La Centrale des caisses de crédit du Canada (CCCC) pense également que ces codes sont préférables à une loi.

La majorité des mémoires présentés par les entreprises de télécommunications et de câblodistribution sous réglementation fédérale indiquent aussi une préférence pour l'autoréglementation de la protection des renseignements personnels. Au sein du secteur bancaire sous réglementation fédérale, l'Ombudsman bancaire canadien (OBC) est moins favorable à l'adoption d'une loi que l'Association des banquiers canadiens (ABC). Dans les autres mémoires émanant de l'industrie, les opinions exprimées sur la nécessité de légiférer vont d'un appui et

d'une acceptation manifestes à une préférence pour les codes volontaires. Parmi les 39 organisations du milieu des affaires ayant présenté un mémoire en réponse au document de travail, 17 sont en faveur de l'adoption d'une loi, 12 sont contre et 6 ont exprimé un point de vue ambivalent.

Quelle que soit leur opinion sur la nécessité d'adopter une loi, pratiquement tous les répondants estiment que la norme de la CSA constitue un bon point de départ. Presque toutes les parties y voient un document qui a fait l'objet d'un consensus, auquel l'industrie, le gouvernement et les groupes de défense des consommateurs ont largement contribué et qu'ils appuient fortement.

Quant à savoir si cette norme doit être adoptée telle quelle ou s'il faut la préciser, les opinions divergent.

Les commissaires, les groupes de défense des consommateurs et la plupart des particuliers préconisent une loi plus précise. Le commissaire à la protection de la vie privée du Canada propose des modifications précises et détaillées au libellé de la norme de la CSA. En revanche, la majorité des organisations du milieu des affaires préféreraient que la norme soit adoptée telle quelle. Elles estiment généralement que la norme de la CSA laisse la souplesse nécessaire aux entreprises et que des exigences plus rigoureuses pourraient nuire aux activités du secteur privé.

Toutefois, les organisations du milieu des affaires ne partagent pas toutes ce point de vue. En réponse à la *question n° 1*, ainsi qu'aux *questions nos 2 et 4*, qui traitent précisément du contenu de la norme de la CSA, plusieurs de ces organisations souhaitent une précision accrue pour ainsi disposer de « règles claires et prévisibles » et obtenir une plus grande certitude sur les aspects qui laissent place à l'interprétation, tout en répondant aux besoins de leur industrie.

Les commentaires des partisans d'une précision accrue portent sur une vaste gamme d'aspects; on peut cependant indiquer que les commissaires, les groupes de défense des consommateurs et les particuliers souhaitent en général des définitions beaucoup plus précises de l'objet visé par la collecte d'information et tiennent à s'assurer que cet objet est légitime. Le recours au consentement tacite, les modalités d'obtention de ce consentement et la façon de protéger les données quand elles sont traitées par des tiers ou à l'extérieur du Canada soulèvent aussi des inquiétudes. Cette question a également suscité des commentaires sur plusieurs aspects de la collecte et de l'utilisation des renseignements personnels, comme la surveillance, le caractère confidentiel du courrier électronique ainsi que la collecte et l'utilisation de données biométriques.

Les points de vue exprimés sur l'utilisation de la norme de la CSA et sur d'autres aspects sont présentés ci-dessous par catégories. Il est à noter que les répondants n'ont pas nécessairement répondu à toutes les questions. Des commentaires figurent dans les réponses à

chaque question uniquement dans les cas où des organisations ou des particuliers ont choisi d'en formuler[1].

Commissaires

Le commissaire à la protection de la vie privée du Canada, les commissaires à l'information et à la protection de la vie privée de l'Alberta, de la Colombie-Britannique et de l'Ontario ainsi que la Commission d'accès à l'information du Québec (Commission d'accès) ont présenté des mémoires.

Tous les commissaires sont favorables à l'adoption d'une loi sur la protection des renseignements personnels, mais ils estiment que la norme de la CSA doit faire l'objet d'améliorations considérables pour servir de base à la nouvelle loi.

Le commissaire fédéral a formulé des commentaires précis sur chacun des dix principes de la norme de la CSA. Son mémoire a été le seul à proposer des modifications précises du libellé de cette norme. Voici ses principaux commentaires :

- Sous la rubrique *Responsabilité*, ajouter une disposition précisant que les organisations sont juridiquement responsables des renseignements qu'elles remettent à des tiers pour que ceux-ci les utilisent en leur nom.

- Sous la rubrique *Détermination de l'objet de la cueillette des renseignements*, ajouter une disposition indiquant qu'il faut, avant même de recueillir tout renseignement personnel, évaluer et documenter l'objet de la cueillette (qui doit être légitime) et informer le particulier de cet objet, de la nature obligatoire ou volontaire de son consentement, des conséquences du refus d'accorder son consentement, des destinataires de l'information et de son utilisation.

- Sous la rubrique *Consentement*, ajouter une disposition précisant que le consentement doit être expliqué de façon complète et claire, donné de façon libre, éclairée, précise et explicite pour tous les modes d'utilisation de l'information et pour tous les destinataires éventuels et autorisé pour une durée limitée.

---

[1] Dans de nombreux cas, le point de vue exprimé par l'organisation ou le particulier sur des questions précises est ambigu et il n'a pas alors été possible de leur attribuer une opinion clairement définie. En pareil cas, le point de vue n'est généralement pas reproduit ici. En outre, l'organisation ou le particulier a parfois proposé un modèle de réglementation de la protection des renseignements personnels sans lien avec certaines questions. Au lieu de tenter d'adapter le modèle à la question, nous avons omis de présenter ici certains commentaires, qui figurent toutefois dans le mémoire visé.

- Sous la rubrique *Limitation de la collecte*, ajouter une disposition indiquant que la collecte de renseignements personnels est limitée aux cas où la loi l'exige ou à des fins indiquées de façon précise et qu'elle doit se faire directement auprès de la personne visée, sauf lorsque la santé et la sécurité sont directement menacées ou qu'elle est exigée par la loi.

- Sous la rubrique *Limitation de l'utilisation, de la communication et de la conservation*, ajouter une disposition précisant que les renseignements personnels peuvent être utilisés ou divulgués uniquement aux fins précises pour lesquelles ils ont été recueillis et avec le consentement de la personne visée, sauf lorsque la santé et la sécurité sont menacées ou que la loi l'exige, que l'on ne peut divulguer ces renseignements sans prendre des mesures comparables de sécurité, et que l'on doit les conserver uniquement pendant la période nécessaire pour l'objet visé et les détruire ensuite de façon sûre. Il faut assurer la confidentialité de tous les renseignements personnels et les communiquer uniquement à ceux qui ont besoin d'en prendre connaissance. En outre, une entente de non-divulgation doit avoir été conclue pour les tiers. On ne doit en aucun cas divulguer des renseignements personnels sans que la personne visée en soit informée ou qu'elle ait donné son consentement, à moins que leur divulgation soit exigée par la loi.

- Sous la rubrique *Exactitude*, remplacer l'expression « utilisés » par « utilisés ou divulgués ».

- Sous la rubrique *Mesures de sécurité*, ajouter une disposition indiquant que les organisations et leurs mandataires doivent protéger les renseignements personnels en prenant des mesures de sécurité matérielles, administratives et techniques contre l'accès accidentel ou non autorisé, la modification ou la destruction.

- Sous la rubrique *Transparence*, remplacer l'expression « efforts déraisonnables » par « coûts ou efforts déraisonnables » et ajouter que les organisations doivent fournir des renseignements précis sur leur gestion des renseignements personnels ainsi que sur leurs politiques et leurs pratiques en matière de règlement des plaintes.

- Sous la rubrique *Accès aux renseignements personnels*, remplacer la formulation du principe par le texte suivant : « On doit informer toute personne qui en fait la demande de l'existence de renseignements personnels la concernant, de l'utilisation qui en est faite ainsi que de leur divulgation et lui permettre d'avoir accès à ses renseignements sans coûts ou efforts déraisonnables, sauf dans les cas prévus par la loi. Le particulier peut contester l'exactitude et l'exhaustivité des renseignements et les faire modifier, mettre à jour ou supprimer selon les circonstances. Il faut répondre dans les délais prévus aux demandes d'accès aux renseignements, de correction, de modification et de suppression. »

- Sous la rubrique *Possibilité de porter plainte contre le non-respect des principes*, ajouter une disposition indiquant que les organisations doivent donner suite aux contestations

dans les délais prévus et que le particulier insatisfait de la réponse d'une organisation peut en appeler auprès d'un organisme central de surveillance.

Le commissaire à l'information et à la protection de la vie privée de l'Alberta est d'avis que le consentement tacite ne cadre pas avec les pratiques équitables en matière d'information et recommande que la loi précise qu'il s'agit d'un consentement écrit. Il ajoute que la loi doit exiger que le particulier en soit informé lorsque des renseignements sont transmis à un tiers sans son consentement.

Le commissaire de Colombie-Britannique estime que la norme de la CSA ne peut servir de base à la loi et il demande au gouvernement de s'inspirer des dispositions beaucoup plus rigoureuses sur la protection de l'information de la *Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1996 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (Directive de l'Union européenne) et de la *B.C. Freedom of Information and Protection of Privacy Act.*

Le commissaire de l'Ontario recommande pour sa part d'insérer dans la loi un article liminaire permettant de mieux définir l'objet de la collecte et de préciser davantage les fins acceptables à cet égard de manière à resserrer et à consolider le principe de la *limitation de la collecte* de la norme de la CSA.

La Commission d'accès estime que l'on aurait avantage à s'inspirer de la loi 68, *Loi sur la protection des renseignements personnels dans le secteur privé en vigueur* au Québec, plutôt que sur la norme de la CSA, pour rédiger la nouvelle loi.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

Au total, les groupes de défense des consommateurs et de l'intérêt du public, notamment le Syndicat canadien de la fonction publique (SCFP), ont présenté 11 mémoires. Toutefois, le nombre de groupes de défense des consommateurs et de l'intérêt public représentés par ces mémoires est beaucoup plus élevé.

Le Centre pour la promotion de l'intérêt public de la Colombie-Britannique a formulé des commentaires au nom de neuf autres organisations de Colombie-Britannique, connues sous le nom de BCOAPO (*se reporter à la Liste des mémoires pour connaître l'identité de ces groupes*). La Fédération nationale des associations de consommateurs du Québec (FNACQ) et Option consommateurs (OC) ont présenté un mémoire conjoint. Par ailleurs, un groupe du nom de Forum sur la vie privée a présenté un mémoire faisant état des résultats d'une enquête électronique réalisée conjointement par sept organisations.

Toutes les organisations de défense des consommateurs souhaitent que le gouvernement fédéral adopte une loi sur la protection des renseignements personnels dans le secteur privé, mais

aucune n'estime que la norme de la CSA constitue actuellement un point de départ suffisant à cet égard.

La B.C. Civil Liberties Association (BCCLA) pense qu'il faut intégrer à la norme de la CSA un nouveau principe de justification de manière à limiter la collecte d'information aux motifs légitimes et exiger que les organisations justifient leurs motifs si ceux-ci sont contestés. La BCCLA renvoie à l'« intérêt sérieux et légitime » de l'article 4 de la loi du Québec et aux « finalités légitimes » de l'article 6 de la Directive de l'Union européenne, qui constituent à ses yeux des précédents pour le principe de justification. La BCCLA ajoute que la loi sur la protection des renseignements personnels doit également s'appliquer à l'intrusion dans la vie privée, en précisant que les pratiques de certaines organisations, comme les tests de dépistage obligatoire des drogues en milieu de travail, contreviennent à la notion de protection de la vie privée, même si aucun renseignement personnel n'est recueilli au bout du compte.

La B.C. Freedom of Information and Privacy Association (FIPA) appuie le principe de la justification et ajoute qu'il faut en arriver à incorporer à la *Charte canadienne des droits et libertés* un droit à la protection des renseignements personnels. La Coalition canadienne de l'information publique (CCIP), le Forum sur la vie privée et le Centre pour la promotion de l'intérêt public (CPIP) partagent cette opinion.

La CCIP pense également que la loi doit s'inspirer à la fois de la norme de la CSA et des pratiques équitables en matière d'information dont fait état le document de travail d'Industrie Canada.

L'Association des consommateurs du Canada (ACC) ne souhaite pas que la loi autorise le consentement par défaut, sauf dans les cas pleinement justifiés. Il faut exiger que la raison à l'origine de tout regroupement de données soit indiquée clairement et interdire la prospection de données. L'ACC propose aussi l'addition des 12 principes du code de protection des renseignements médicaux en vigueur en Nouvelle-Zélande.

La section ontarienne de l'Association des consommateurs du Canada (ACC de l'Ontario) souhaite que la loi s'inspire de la norme de la CSA, mais elle ne fait aucun commentaire sur les obligations additionnelles. Le Conseil canadien de la consommation (CCC) est également d'avis que la loi doit s'inspirer de la norme, mais il précise que les particuliers doivent demeurer les seuls propriétaires des renseignements personnels les concernant et avoir le droit d'en contrôler l'utilisation.

La FNACQ et OC estiment que la nouvelle loi sur la protection des renseignements personnels dans le secteur privé peut s'inspirer non seulement de la norme de la CSA, mais aussi de l'ébauche de la Conférence sur l'uniformisation des lois du Canada (CULC) et de la loi du Québec, qui donnent beaucoup plus de détails sur les obligations.

Le Forum sur la vie privée s'oppose aux énoncés d'objectifs vagues ou généraux et affirme que la loi doit définir de façon précise le consentement afin que le particulier sache qu'on lui demande une permission et qu'il comprenne bien comment les données seront recueillies et utilisées. Tous les modes d'utilisation des données s'inscriront dans le cadre d'une disposition prévoyant la participation, avec consentement écrit dans la mesure du possible. La raison invoquée doit être très précise et il ne faut pas refuser d'assurer des services ni imposer d'autres formes de pénalité à une personne refusant de consentir à la collecte non nécessaire de renseignements. On doit limiter clairement la durée d'utilisation des renseignements et obtenir un consentement précis pour échanger des renseignements avec d'autres organisations, affiliées ou non, ou avec d'autres services d'une société. Les renseignements de nature génétique ou médicale doivent bénéficier d'une protection spéciale et ce sont les parents et tuteurs qui doivent en contrôler l'utilisation dans le cas des enfants.

Le Forum sur la vie privée ajoute que la définition des notions de vie privée et de protection des renseignements personnels figurant dans le document de travail doivent être intégrées à la loi. Comme les employés sont souvent les seules personnes au sein d'une organisation à être au courant des cas d'utilisation de l'information à mauvais escient, la loi doit assurer une protection spéciale aux employés qui dénoncent ces cas.

De plus, la CPIP souhaite que la loi renferme une clause privative empêchant les parties de se soustraire à son application. Elle propose également que deux des *principes de protection des renseignements personnels dans le domaine des télécommunications* soient ajoutés au texte de la loi. En vertu de ces principes, il faut non seulement tenir compte explicitement de la protection des renseignements personnels au moment de la prestation de nouveaux services ou de l'introduction d'un nouveau service portant atteinte à la vie privée, mais aussi prendre des mesures appropriées pour protéger les renseignements personnels relatifs aux clients, sans leur imposer un coût supplémentaire, à moins qu'il y ait des raisons impératives de ne pas le faire.

La CPIP demande également que la définition de la notion d'organisation soit resserrée dans la loi afin d'englober l'utilisation des renseignements par des affiliés ou les droits sur les données concernant des particuliers en cas de fusion. Elle ajoute que, à moins que la loi n'impose des restrictions obligatoires importantes aux fins visées par la collecte d'information, les exigences en matière de consentement doivent préciser davantage l'obligation incombant à une organisation d'informer le particulier des divers modes d'utilisation des renseignements le concernant, en particulier quand il s'agit d'un consentement tacite. La loi doit également établir un délai au-delà duquel l'entreprise devra détruire les renseignements personnels à moins de prouver qu'elle en a encore besoin. Quand la relation avec un client se termine, il faut dépersonnaliser ou détruire les données.

Le BCOAPO ajoute qu'il faudra être beaucoup plus précis pour empêcher une organisation d'invoquer à titre de défense l'argument impénétrable qu'elle a usé de son jugement subjectif de bonne foi à l'égard de la norme de la CSA. Il propose que la norme soit d'accorder le consentement par écrit et qu'il doit incomber à l'organisation de faire la preuve que le

consentement a été accordé quand il s'agit d'un consentement tacite. Le BCOAPO ajoute qu'un motif imprécis doit permettre d'invalider un consentement accordé pour la collecte, la conservation ou la communication de renseignements. Il estime que le simple fait de documenter les fins visées constitue un « exercice sans intérêt ».

Pour sa part, le SCFP est d'avis que la loi fédérale doit s'appliquer aux entreprises qui traitent avec l'administration fédérale ou sont sous réglementation fédérale et imposer des règles strictes régissant la passation de marchés pour le traitement de l'information ou les situations dans lesquelles des entreprises privées ont accès à des données de nature délicate. Il ajoute que la loi doit limiter l'utilisation des renseignements personnels sur les travailleurs aux fins précises pour lesquelles ils ont été recueillis et aux raisons directement liées à l'emploi. Toutes les données doivent faire l'objet de mesures de sécurité raisonnables et, s'il s'agit de données médicales, de protections spéciales supplémentaires. Les renseignements personnels sur les travailleurs ne doivent pas pouvoir être transmis à des tiers sans le consentement écrit exprès de la personne, sauf dans les situations d'urgence, lorsque l'exige la loi ou que la relation d'emploi l'impose. Les travailleurs doivent être informés régulièrement des renseignements personnels qu'on détient sur eux.

Le SCFP soulève également des préoccupations particulières concernant les renseignements médicaux en précisant que la loi doit reprendre les principes de la *Loi canadienne sur la santé* régissant les secteurs public et privé, établir une distinction selon que les renseignements sont recueillis dans l'intérêt public ou à des fins commerciales, protéger la vie privée des patients et la confidentialité des renseignements sur leur santé, veiller à ce que les données sur la santé des personnes servent uniquement aux fins pour lesquelles elles ont été recueillies et interdire que des tiers, par exemple, les compagnies d'assurances, les employeurs et les sociétés pharmaceutiques, aient directement accès aux renseignements sur la santé.

Secteur des soins de la santé

IMS Canada (IMS) et l'Association dentaire canadienne (ADC) estiment que la norme de la CSA constitue un bon point de départ, mais l'ADC ajoute qu'il faut aborder le problème de l'autodétermination des dossiers médicaux. L'Institut canadien d'information sur la santé (ICIS) recommande que la loi fasse la distinction entre les données permettant d'identifier la personne, les données ne permettant pas de l'identifier et les données anonymes. Il souhaite également qu'on établisse une distinction selon que les données servent à des fins lucratives ou non. En outre, l'Association des infirmières et infirmiers du Canada (AIIC) tient à ce qu'on aborde la question de l'identification de l'origine des données et à ce qu'on établisse une distinction entre les utilisations à des fins commerciales ou d'intérêt public. Elle ajoute que la loi doit permettre de conserver certains renseignements précis pendant une longue période, en particulier si on peut les rendre anonymes, et qu'elle doit prévoir un moyen de solliciter le consentement de la personne visée pour utiliser ces données à d'autres fins non prévues au départ.

Organisme d'application de la loi

La Gendarmerie royale du Canada (GRC) recommande d'adopter une loi rigoureuse renfermant certains principes de sécurité, y compris l'application de mesures de sécurité pendant toute la durée du cycle de vie de l'information, l'éducation des propriétaires et des utilisateurs de données sur les principes et sur les mesures de sécurité, l'évaluation régulière des mesures de sécurité et des risques, l'exigence selon laquelle les cadres de travail et les conditions de stockage de l'information non traditionnels (par exemple, le télétravail et les services de stockage de données) ne diminuent pas les responsabilités en matière de sécurité des données et l'application uniforme des normes dans les différents systèmes de gestion d'information.

Administrations publiques (y compris l'Union européenne)

Le ministère des Sciences, de la Recherche et de la Technologie de l'information de l'Alberta estime que la loi doit s'inspirer de la norme de la CSA, mais ajoute qu'il sera peut-être nécessaire de se doter d'un cadre législatif distinct en raison des exigences uniques inhérentes à la protection des renseignements personnels dans le domaine de la santé.

Le directeur général de la DG XV (Marché intérieur et Services financiers) de l'Union européenne souhaite également que la loi canadienne pour le secteur privé s'inspire de la norme de la CSA. Il recommande d'y inclure une disposition sur le transfert des données en dehors du Canada.

Instituts

Le Fraser Institute préférerait que la protection des renseignements personnels dans le secteur privé soit régie par la législation actuelle au lieu que l'on mette en place un tout nouveau système de réglementation. La violation de la protection des renseignements personnels doit donner lieu à des poursuites pour vol et à de lourdes sanctions immédiates. Il faut s'en remettre aux tribunaux pour assimiler aux lois existantes le vol de renseignements personnels.

Le Centre de recherche et d'enseignement sur les droits de la personne de l'Université d'Ottawa (Centre de l'Université d'Ottawa) demande que la loi tienne compte de plusieurs recommandations de la charte proposée pour la protection des renseignements personnels dans le rapport intitulé *La vie privée – où se situe la frontière*, émanant du Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre des communes. Ces recommandations précisent que toute personne est de plein droit propriétaire des renseignements personnels la concernant, qu'elle a le droit de s'attendre à l'anonymat et d'en bénéficier à moins que des motifs raisonnables justifient le besoin d'identifier des particuliers, et que le non-respect des droits de protection des renseignements personnels doit être autorisé uniquement à titre exceptionnel si cette mesure est raisonnable et que l'on peut en prouver le bien-fondé. Toujours selon le Centre, la loi doit préciser que les renseignements peuvent être recueillis uniquement à des fins raisonnables dont la justification peut être démontrée. Il propose par ailleurs que l'on

présente dans la loi la définition des notions de vie privée et de protection des renseignements personnels qui figure dans le document de travail d'Industrie Canada et de Justice Canada.

Associations d'archivistes, d'historiens et de bibliothécaires

Le Comité canadien des affaires législatives et réglementaires d'ARMA International estime que l'expression « à moins qu'il ne soit pas approprié de le faire » sous la rubrique « Consentement » (*troisième principe*) de la norme de la CSA accorde une trop grande liberté de manœuvre aux gestionnaires d'information et qu'elle risque de susciter des différends avec les consommateurs. Le Comité canadien des affaires législatives et réglementaires est aussi d'avis que l'obligation de conserver l'information uniquement pendant la durée nécessaire pour atteindre l'objectif défini (*cinquième principe*) est trop vague car elle ne précise pas les objectifs qui l'emportent au moment de déterminer la période de conservation de renseignements. De même, l'expression « que la loi ne l'exige » ne s'applique pas de façon adéquate à tous les cas. Le Comité canadien des affaires législatives et réglementaires juge que l'obligation d'informer les particuliers de l'existence, de l'utilisation et de la divulgation de renseignements personnels les concernant et de leur y donner accès (*neuvième principe*) est inappropriée car elle va au-delà du droit d'accès déjà prévu dans la *Loi sur la protection des renseignements personnels* et dans les lois provinciales équivalentes, qui prévoient des exceptions précises à ce droit d'accès.

L'Association des archivistes du Québec (AAQ) estime que la loi doit permettre à la société de conserver sa « mémoire collective » en autorisant la divulgation et l'utilisation de renseignements personnels à des fins de recherche, sans avoir à obtenir de consentement, comme le permettent la *Loi sur la protection des renseignements personnels* et la Directive de l'Union européenne, pour autant que la personne visée ne subisse aucun préjudice. En outre, la loi doit autoriser les entreprises à transmettre des renseignements personnels présentant un intérêt historique à tout service d'archives sans le consentement du particulier visé. L'organisme recevant les renseignements personnels doit être tenu de les détruire lorsqu'ils ne lui sont plus utiles.

La Société historique du Canada (SHC) et l'Institut d'histoire de l'Amérique française (IHAF) souhaitent que la loi tienne compte des questions de patrimoine. Ces organismes s'inquiètent de l'apparition de la notion de finalité dans l'utilisation des données, qui débouche ensuite sur leur destruction. D'après les deux organismes, la loi ne doit ni réduire la capacité des archivistes à recueillir et à conserver les collections de données ainsi qu'à les mettre à la disposition des chercheurs qualifiés, ni limiter la durée de vie des données nécessaires aux recherches historiques.

L'IHAF ajoute que la législation doit limiter la durée de la protection de l'information, déterminer de façon explicite que les renseignements personnels sont également des données d'archives et reconnaître le rôle des établissements et des organismes de protection du patrimoine dans la conservation de cette information.

L'Ontario Library Association (OLA) demande que la loi soit conforme à la Directive de l'Union européenne.

Secteur des télécommunications et de la câblodistribution

Neuf mémoires ont été présentés par des organismes du secteur des télécommunications et de la câblodistribution sous réglementation fédérale. Il s'agissait des Entreprises AT&T Canada (AT&T), d'un mémoire collectif d'ACC TelEnterprises Inc., d'AT&T Canada Services interurbains, de Call Net Enterprises Inc., de fONOROLA Inc. et de Westel Telecommunications Ltd. (regroupement de fournisseurs de services de télécommunications), de la Fondation des normes de télévision par câble (FNTC), de l'Association canadienne de télévision par câble (ACTC), de l'Association canadienne des télécommunications sans fil (ACTS), de Microcell Communications Inc. (Microcell), de Rogers Communications Inc. (Rogers), de Stentor Politiques publiques Télécom inc. (Stentor), qui a formulé des commentaires au nom de la plupart des entreprises membres de Stentor, et de TELUS.

Parmi ces entreprises, seules l'ACTS et Microcell préconisent ouvertement l'adoption d'une loi.

Toutes les organisations ont cependant indiqué que la norme de la CSA constitue le point de départ approprié si l'on adopte une nouvelle loi. Exception faite de Microcell, qui propose de préciser le libellé de la norme, toutes sont favorables à l'utilisation de la norme telle quelle.

Le regroupement de fournisseurs de services de télécommunications signale cependant que le ministre de l'Industrie devrait donner des directives au CRTC afin que celui-ci élimine les dispositions sur le caractère confidentiel des renseignements sur les consommateurs des conditions régissant les services offerts par les fournisseurs de télécommunications car elles estiment que ces dispositions ne sont pas compatibles avec la norme de la CSA.

Stentor ajoute par ailleurs que la loi doit prévoir une période de transition afin de permettre aux entreprises de préparer des codes adaptés au nouveau libellé et de mettre en place les pratiques nécessaires pour prendre en charge à la fois les renseignements personnels déjà recueillis et à ceux qui le seront ultérieurement.

Secteur financier

Les mémoires du secteur financier provenaient à la fois d'organisations sous réglementation fédérale et provinciale, comme des banques, des compagnies d'assurances, des organismes de réglementation du marché des valeurs mobilières, des bourses, des comptables et des organisations représentant les intérêts de professionnels œuvrant dans ce secteur défini au sens large.

L'ABC préconise l'adoption d'une loi peu contraignante, souple et efficace s'inspirant de la norme de la CSA. Elle précise que cette norme devrait, dans sa forme actuelle, être intégrée au libellé de la loi plutôt que d'y faire l'objet d'un renvoi. Quant à lui, l'OBC n'est pas favorable à l'adoption d'une loi sur la protection des renseignements personnels dans le secteur privé, mais il estime que le modèle de la CSA doit être reconnu à titre de norme législative pour la protection des renseignements personnels, comme c'est le cas pour les principes comptables généralement reconnus, qui constituent pour l'industrie une norme obligatoire ayant force de loi.

Le Canada Trust et l'Association des compagnies financières canadiennes (ACFC) sont en faveur de l'adoption d'une loi s'inspirant de la norme de la CSA. L'ACFC précise qu'il vaut mieux préciser les obligations en détail dans les codes sectoriels, alors que le Canada Trust estime que des obligations additionnelles provoqueraient un déséquilibre entre les intérêts des diverses parties. L'ACFC et l'Association canadienne des compagnies d'assurance de personnes (ACCAP) préconisent également l'adoption d'une loi qui serait fondée sur la norme de la CSA, sans imposer d'obligations additionnelles. L'Association canadienne des institutions financières en assurance (ACIFA) signale que, à l'ère de l'électronique, il faut tenir compte du besoin de souplesse pour l'obtention du consentement.

Le Conseil d'assurances du Canada (CAC) et Equifax Canada (Equifax) ne sont pas favorables à l'adoption d'une loi. Le CAC précise que l'industrie des assurances multirisques fait un bon travail en matière d'autoréglementation. Equifax ajoute que les faits observés ne donnent pas à penser que les codes volontaires sont inadéquats ou qu'ils le seront. La CCCC préfère aussi l'application volontaire de codes sectoriels. Toutefois, les trois organisations estiment que la norme de la CSA, dans sa forme actuelle, constitue un bon point de départ si on juge vraiment nécessaire de se doter de ce type de loi.

La Certified General Accountants Association of Ontario (CGA Ontario) est favorable à l'adoption d'une loi fondée sur la norme de la CSA, mais ajoute qu'elle doit être plus détaillée. Elle propose que la loi donne des conseils plus précis en matière de consentement dans le cas des renseignements de nature délicate et qu'elle offre des possibilités de retrait positif dans le cas de renseignements non essentiels. CGA Ontario souhaite également que l'on précise les règles à appliquer dans le cas où l'utilisation ou la divulgation ultérieures de renseignements seraient conformes aux fins visées à l'origine et comprises dans le consentement donné au début. Elle ajoute que le principe relatif à l'accès aux renseignements personnels inhérent à la norme de la CSA est vague dans le cas des dérogations au droit d'accès, des délais prévus, des frais pouvant être facturés et des circonstances dans lesquelles les entreprises peuvent être tenues de transmettre à des tiers des avis de correction de renseignements personnels.

CGA Ontario demande également qu'il soit interdit de recueillir et de conserver des renseignements de nature délicate, par exemple, sur le point de vue en matière politique ou religieuse, l'adhésion à un syndicat, la race, la santé ou la vie sexuelle sans besoin légitime ou sans mesures de sécurité appropriées, même si la collecte de renseignements de nature financière exigés par les entreprises ne doivent pas être soumis à ces restrictions. Elle ajoute en outre qu'il

doit revenir au particulier de décider si les renseignements personnels sont utilisés à des fins autres que celles prévues à l'origine et que la nouvelle loi doit contenir des dispositions précises sur le consentement et sur l'utilisation des renseignements personnels quand il s'agit d'assurer un marketing ciblé, de faire la prospection de données et d'atteindre d'autres objectifs non reliés aux premiers.

Les employés de Deloitte et Touche (employés de Deloitte) sont également favorables à l'adoption d'une loi s'inspirant de la norme de la CSA, mais souhaitent une loi plus précise en ce qui concerne les principes de mesures de sécurité et de transparence. Sous la rubrique « Mesures de sécurité », il faut étoffer les renvois aux mesures techniques en exigeant précisément que le niveau de sécurité soit fonction du caractère délicat de l'information et que la viabilité des mesures de sécurité soit évaluée sur une base permanente. Les employés de Deloitte proposent également que les organisations soient tenues d'adapter les méthodes de communication de renseignements en fonction des politiques des entreprises en matière de protection des renseignements personnels ainsi que de la méthode de demande et font valoir que le fait d'autoriser des organisations à répondre par la poste à des demandes transmises en direct entre en contradiction avec l'objectif du principe d'accès aux renseignements personnels compte tenu des nouvelles technologies.

Un mémoire du cabinet de comptables agréés Bennett Gold ne s'intéresse pas au contenu du document de travail d'Industrie Canada, mais affirme que le gouvernement doit adopter à titre de mécanisme de vérification et d'attestation pour le commerce électronique au Canada la procédure CA WebTrust, mise au point par l'Institut canadien des comptables agréés et l'American Institute of Certified Public Accountants. M. Gold affirme également que les comptables agréés qui ont suivi la formation nécessaire et sont titulaires d'une licence doivent être autorisés à procéder à des vérifications et à des attestations portant sur le commerce électronique et la protection des renseignements personnels.

Organisations commerciales (y compris les commerces de détail)

L'Association canadienne du marketing direct (ACMD), Enlogix Inc. (Enlogix) et la Chambre de commerce du district de Sudbury préconisent l'adoption d'une loi s'inspirant de la norme de la CSA, sans réclamer de précisions ni d'obligations additionnelles. Enlogix signale cependant que les organisations doivent être tenues de publier des documents résumant leur expérience dans le domaine du traitement des plaintes et de conserver les dossiers de plaintes aux fins de vérification.

L'ACG s'oppose à l'adoption d'une loi, ajoutant que la loi proposée ne doit pas entrer en contradiction avec les lois sur la concurrence, ni établir de limite de temps pour la conservation des données, ni limiter les objectifs visés par l'utilisation de l'information. L'ACG signale que l'industrie du gaz doit recueillir et utiliser des données sur les consommateurs pour les besoins de sa planification dans une perspective de 20 ans. En outre, elle souhaite que toute loi soit

examinée périodiquement (au moins tous les cinq ans), comme le prévoient les articles 88 et 89 de la loi du Québec.

Dun & Bradstreet Canada (D&B) déplore que la norme de la CSA n'établisse pas de règles claires et prévisibles et qu'elle soit trop restrictive dans certains domaines. L'entreprise signale également que la norme de la CSA est plus contraignante que la Directive de l'Union européenne quant aux limites imposées à l'égard de l'utilisation et de la divulgation de l'information. D&B fait remarquer que des règles trop restrictives empêcheraient la divulgation d'information présentant un intérêt légitime pour le milieu des affaires, par exemple, les renseignements sur les procédures de faillite.

L'ACJ craint les répercussions de la norme de la CSA dans le domaine journalistique, car les organisations considèrent que la norme impose un fardeau considérable sur les processus rédactionnels, crée une incertitude quant à sa portée et à son application en ce qui touche la conformité des médias et porte atteinte à l'indépendance éditoriale. Elle ajoute que la loi doit être en harmonie avec la *Déclaration universelle des droits de l'homme*, qui garantit la liberté d'expression des médias et leur droit « de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées ».

Associations du secteur de la technologie de l'information

ACT Canada estime que la norme de la CSA est logique et facile à comprendre, mais qu'il faut la comparer avec la Directive de l'Union européenne et les codes provinciaux de la protection de la vie privée et utiliser la norme la plus rigoureuse. L'ACTP, l'ACFI et l'ACTI sont toutes favorables à une loi s'inspirant de la norme de la CSA dans sa forme actuelle. L'ACFI précise cependant que la loi doit préciser quelles parties sont tenues de répondre des violations de la loi sur la protection des renseignements personnels, en indiquant que les fournisseurs de services Internet ne doivent pas être tenus responsables de la divulgation de renseignements personnels par leurs clients ou de la divulgation accidentelle de renseignements personnels découlant de la collaboration avec des organismes d'application de la loi.

L'Association canadienne de l'informatique (ACI) estime que la norme de la CSA doit fournir davantage de précisions sur la prospection de données par intrusion et lors d'interconnexion d'ordinateurs, que la norme ne précise pas suffisamment les exigences en matière de tenue de registres quand les données sont divulguées à des tiers, qu'elle passe sous silence les transferts transfrontaliers de données et qu'elle peut permettre l'obtention d'un consentement tacite pour camoufler des pratiques intrusives adoptées par des spécialistes de la commercialisation, qui, sans être trompeuses, n'informent pas pleinement.

Particuliers (y compris les consultants, les experts et les universitaires)

La question a soulevé énormément de commentaires de la part des 22 particuliers qui y ont répondu. Tous, à l'exception d'un, estiment que la norme de la CSA constitue le meilleur

point de départ. Aucun n'a jugé la norme suffisante dans sa forme actuelle. Les modifications proposées sont très variées, par exemple :

- Ajouter un principe de justification de la collecte des renseignements.

- Ajouter deux principes de la charte proposée sur la protection des renseignements personnels figurant dans le document *La vie privée: où se situe la frontière*, en précisant qu'il faut limiter la collecte de renseignements aux cas où elle est nécessaire et justifiable dans les circonstances et veiller à pénaliser les personnes qui ont choisi d'exercer leur droit à la protection des renseignements personnels les concernant.

- Incorporer les principes n^{os} 6, 7, 8, 10, 17 et 18 de la charte sur la protection des renseignements personnels en vigueur en Australie, principes relatifs à l'absence de surveillance, à la protection des communications, à l'espace privé, aux transactions anonymes, aux registres publics et à l'interdiction de pénaliser en cas de refus de divulgation.

- Incorporer un principe de protection des renseignements personnels dans le domaine des télécommunications, selon lequel la mise en œuvre de technologies envahissantes doit s'accompagner de politiques permettant de protéger les renseignements personnels sans coût additionnel pour le consommateur.

- Retenir les dispositions qui concernent l'équité dans ce domaine apparaissant dans la loi du Québec.

- Exiger que l'on informe les particuliers des pratiques de gestion des renseignements ainsi que des mécanismes de recours.

- Exiger que les mandataires ou les filiales accordent l'accès à l'information directement plutôt que par l'intermédiaire de l'organisation dont ils relèvent.

- Exiger que les entreprises informent les particuliers de leur gamme d'activités, de leurs agences et de leurs filiales.

- Exiger que les entreprises partagent l'information avec leurs mandataires, leurs filiales et des tiers pour que l'information soit aussi exacte que si elle avait été fournie par l'entreprise principale.

- Veiller à ce que la loi régisse tous les modes d'utilisation des renseignements personnels par les particuliers, les entreprises, les organismes, les groupes sans but lucratif, les Églises, les syndicats, les groupes d'action politique et d'intérêt et les autres intervenants.

- Préciser les dispositions sur le consentement, en accroissant les exigences relatives au consentement tacite et en limitant davantage le recours au consentement par défaut.

- Exiger la possibilité de retrait pour tous les modes d'utilisation à des fins de marketing non essentiels.

- Exiger le consentement des parents pour la collecte et l'utilisation de renseignements sur les enfants.

- Limiter la collecte d'information au minimum absolument nécessaire (ce qui éliminerait la collecte d'information à titre gratuit).

- Préciser que l'information ne peut être recueillie que directement auprès du particulier.

- Préciser que la collecte indirecte d'information doit être autorisée uniquement dans de très rares cas, qu'elle doit toujours être documentée, sauf dans les circonstances où elle s'inscrit dans le cadre de l'application de la loi.

- Déterminer une période minimale de conservation des données pour tout renseignement personnel (au moins de six mois à un an après la dernière utilisation).

- Préciser que, quand on corrige une information, il faut détruire tous les renseignements recueillis de façon accidentelle ou involontaire non essentiels aux activités.

- Quand une entreprise refuse de modifier, d'ajouter ou de supprimer de l'information, exiger qu'une demande de correction et une liste des tiers à qui l'information a été communiquée au cours des deux années antérieures soient jointes aux renseignements contestés.

- Ajouter un renvoi aux normes assurant la conservation et l'élimination sûres de l'information.

- Ajouter des restrictions et des mécanismes de protection spéciaux concernant l'utilisation des données biométriques.

- Instituer un droit à l'autodétermination pour les dossiers médicaux (en s'appuyant sur la décision de la Cour suprême dans *McInerney c. MacDonald*), ce droit étant inaliénable et s'appliquant quel que soit l'endroit où l'information est stockée afin d'imposer aux organisations qui gèrent les banques de données des responsabilités accrues en matière de conservation.

- Interdire la collecte d'identificateurs uniques, sauf quand cette mesure est expressément prévue par la loi.

- Interdire le transfert de renseignements personnels vers d'autres pays sans protection adéquate.

- Exiger un contrat tenant les organisations canadiennes responsables de la divulgation de renseignements personnels en dehors du Canada.

- Veiller à ce que toutes les technologies et tous les programmes d'échange d'information ainsi que leurs objectifs soient approuvés par le gouvernement.

- Exiger que les entreprises assurant des services aux administrations publiques soient soumises aux mêmes obligations que ces administrations et à la loi sur la protection des renseignements personnels dans le secteur privé.

- Prévoir une protection contre les divers types de frais qui pourraient empêcher d'avoir accès aux renseignements personnels en temps utile.

- Interdire la transmission clandestine et l'interception de renseignements sans le consentement des deux parties ou une autorisation d'un tribunal.

- Exiger que les organisations fournissent gratuitement les listes résumant les renseignements personnels qu'elles utilisent pour fournir des services ou prendre des décisions, ainsi qu'un barème de prix pour montrer les coûts réels qu'entraîne l'accès complet aux renseignements personnels.

- Interdire la surveillance, sauf aux fins de l'application de la loi.

- Étendre au courrier électronique les protections juridiques s'appliquant aux télécommunications vocales.

- Faire de la transmission abusive de publicités électroniques à des personnes qui ne souhaitent pas les recevoir une violation de la loi comparable à la fraude postale.

- Faciliter la protection des renseignements personnels au moyen du chiffrement à clé publique afin d'empêcher la contrefaçon des en-têtes de courrier.

Faits saillants

Les répondants reconnaissent généralement que la loi doit s'inspirer de la norme de la CSA. Toutefois, au moment de la rédaction de la loi, il faudra tenir compte des commentaires formulés par les diverses parties, y compris les commissaires à l'information et à la protection de la vie privée, les groupes de défense des consommateurs, les organisations du milieu des affaires, les groupes d'intérêt et les particuliers, relativement à la nécessité d'une précision accrue et d'obligations supplémentaires.

2. Dans quelles circonstances la loi doit-elle permettre la divulgation de renseignements personnels à une tierce partie sans le consentement de l'intéressé? Quelles conditions devraient s'appliquer?

La plupart des parties ayant formulé des commentaires sur la question estiment que la loi doit permettre la divulgation des renseignements personnels sans consentement quand il s'agit de l'application de la loi ou de situations d'urgence médicale, ainsi que dans les rares circonstances impérieuses où la personne n'est pas en mesure de fournir les renseignements qui la concernent. Mentionnons notamment les cas de risques pour la santé ou la sécurité, de risques de blessures pour autrui ou pour soi ou encore les cas où la divulgation est absolument essentielle aux entreprises (par exemple, comme l'ont fait valoir les compagnies de téléphone, ceux où il faut divulguer des renseignements personnels pour assurer le fonctionnement efficace des réseaux de télécommunications). Le mémoire du commissaire à l'information et à la protection de la vie privée de l'Alberta et celui d'un autre intervenant proposent également que les risques environnementaux soient considérés comme une raison légitime d'autoriser la divulgation de renseignements sans consentement.

Sur la question de l'utilisation des renseignements personnels à des fins de recherche médicale, des répondants ont indiqué que les renseignements doivent être divulgués uniquement si le particulier peut en retirer un avantage direct ou s'il est manifeste que la recherche est d'intérêt public. Ils sont peu favorables à la divulgation sans consentement de renseignements médicaux permettant d'identifier la personne visée, sauf dans de rares circonstances. Les répondants estiment qu'il faut exiger l'approbation de la personne visée ou de l'organisme de surveillance pour toute divulgation, à des fins de recherche ou dans l'intérêt public, de renseignements permettant d'identifier une personne.

Les archivistes souhaitent qu'une exemption soigneusement définie soit accordée à l'égard des exigences de consentement pour les documents de nature historique, alors que l'ACJ insiste beaucoup sur la nécessité de divulguer des renseignements sans consentement pour le matériel journalistique.

Selon un grand nombre d'intervenants du secteur privé, la norme de la CSA dans sa forme actuelle est suffisante. D'autres souhaitent une clarté accrue pour le traitement de plusieurs cas particuliers, par exemple, le recouvrement et la prévention de dettes, ainsi que, dans le cas des compagnies de téléphone, pour des besoins commerciaux précis, comme la reconquête de clients.

Les câblodistributeurs et les fournisseurs de services Internet veulent que la loi les dégage de toute responsabilité lorsque l'information est divulguée par un membre du public utilisant leurs installations et qu'ils n'exercent aucun contrôle direct sur elle.

Les entreprises qui recueillent et utilisent des renseignements commerciaux et accessibles à tous sur des particuliers veulent que cette information puisse être divulguée

sans consentement, faisant valoir que cette pratique est souvent dans l'intérêt du public, c'est-à-dire, par exemple, que la divulgation de renseignements sur les procédures de faillite relève de l'intérêt public. Par ailleurs, les organismes de réglementation, comme ceux qui réglementent le marché des valeurs mobilières, veulent pouvoir recueillir et utiliser des renseignements sans consentement pour assurer l'intégrité des marchés financiers.

Le secteur des assurances a mentionné qu'il relève de la responsabilité publique de divulguer sans consentement des renseignements utiles aux pouvoirs publics pour la réalisation d'objectifs publics.

À l'opposé de ces divers exemples, les groupes de défense des consommateurs veulent en général que l'on impose des limites strictes quant à la divulgation de renseignements sans consentement. Dans le contexte du journalisme, la divulgation sans consentement ne recueille qu'un appui mitigé. En outre, certains répondants ont proposé que les organisations soient tenues de documenter et de justifier toute divulgation de renseignements sans consentement. On trouvera ci-après un aperçu des divers points de vue exprimés dans les mémoires.

Commissaires

Le commissaire à la protection de la vie privée du Canada est d'avis que la divulgation de renseignements sans consentement ne doit être permise que dans les cas où la santé et la sécurité d'un particulier sont menacées ou quand la loi l'exige.

Le commissaire à l'information et à la protection de la vie privée de l'Alberta propose que la divulgation de renseignements sans consentement soit autorisée pour assurer l'application de la loi, pour protéger la santé et la sécurité d'un particulier ainsi que pour communiquer de l'information sur un risque pour l'environnement, pour la santé et la sécurité du public ou des renseignements dont la divulgation est manifestement dans l'intérêt du public.

Les commissaires de la Colombie-Britannique et de l'Ontario préconisent tous deux que l'on établisse des conditions limitées et très bien définies pour la divulgation de renseignements sans consentement. Quant à la Commission d'accès, elle préfère le libellé de la loi du Québec.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

Tous les groupes qui ont formulé des commentaires sur la question estiment que les renseignements personnels ne doivent pratiquement jamais être diffusés sans consentement, sauf dans le cas où il s'agit de l'application de la loi, dans les cas d'urgence ou présentant des

risques pour la santé et la sécurité lorsqu'il y va de l'intérêt public, défini clairement dans son sens étroit. La FIPA ajoute qu'il faudrait faire la preuve de la probabilité de préjudice.

Le CPIP souligne que la loi doit également aborder la question de la divulgation de renseignements du domaine public sans consentement.

Secteur des soins de la santé

L'ADC estime que la loi doit permettre la divulgation de renseignements sans consentement dans des cas précis concernant la santé si un praticien du secteur a des raisons de croire que le comportement d'un patient peut avoir des effets néfastes (par exemple, dans le cas d'un patient atteint d'une maladie transmise sexuellement). En pareil cas, il faut diffuser uniquement les données strictement nécessaires.

L'AIIC pense que les renseignements doivent pouvoir être divulgués sans consentement uniquement lorsque le particulier en retire un avantage direct ou que leur divulgation est manifestement dans l'intérêt public, par exemple, pour les besoins de recherches. Pour sa part, l'ICIS juge que les données concernant précisément une personne doivent pouvoir être divulguées sans consentement uniquement dans des cas très précis. Enfin, IMS estime qu'aucune démarche visant à définir les circonstances exceptionnelles ne permettra de couvrir toutes les possibilités et souhaite qu'on conserve l'expression « jugé approprié » figurant dans le *troisième principe* et qu'il soit ajouté aux *quatrième et cinquième principes* de la norme de la CSA.

Organisme d'application de la loi

La GRC est d'avis qu'il faut exiger un consentement éclairé pour la divulgation de renseignements, ou à tout le moins que les particuliers doivent avoir été informés que des renseignements les concernant peuvent être divulgués dans des conditions précises et limitées.

Elle ajoute que le cadre législatif doit permettre la communication de renseignements aux organismes d'application de la loi et aux autres organismes d'enquête du gouvernement (par exemple, les Douanes, le Bureau de la concurrence et Revenu Canada) en vertu de l'article 8 de la *Loi sur la protection des renseignements personnels* dans sa forme actuelle, qui permet sans consentement la « communication à un organisme d'enquête déterminé par règlement qui en fait la demande par écrit, en vue de faire respecter des lois fédérales ou provinciales ou pour la tenue d'enquêtes licites, pourvu que la demande précise les fins auxquelles les renseignements sont destinés et la nature des renseignements demandés ».

Instituts

Le Centre de l'Université d'Ottawa recommande que la définition de consentement précise que chacun possède un droit inaliénable de propriété des renseignements personnels le concernant, quel que soit l'endroit où ils sont stockés.

Associations d'archivistes, d'historiens et de bibliothécaires

L'AAQ recommande l'adoption d'une disposition exigeant le consentement pour l'utilisation de renseignements personnels de nature délicate pendant 20 ans à compter de la date de création d'un document et pendant 75 ans pour les renseignements personnels de nature délicate. À l'expiration du délai prévu, les particuliers pourraient également demander une autorisation écrite leur permettant d'assurer la confidentialité des renseignements personnels les concernant pendant une période maximale de 100 ans à compter de la date de création du document.

Le Comité canadien des affaires législatives et réglementaires recommande que les lignes directrices pour la divulgation de renseignements sans consentement s'inspirent de la *Loi sur l'accès à l'information et la protection de la vie privée* de l'Ontario et de la *Loi sur la protection des renseignements personnels* du Canada. L'OLA souhaite que la divulgation de renseignements personnels sans consentement soit autorisée uniquement dans des circonstances précises, par exemple, lorsque la santé ou la sécurité d'une personne sont menacées ou que tous les éléments permettant d'identifier la personne ont été supprimés.

La SHC juge que les règles régissant la divulgation de renseignements sans consentement doivent tenir compte du problème de l'accès dans une perspective historique aux renseignements personnels concernant des personnes décédées. D'après l'IHAF, l'obtention d'un consentement, la limitation de la collecte, de l'utilisation, de la conservation et de la divulgation de renseignements personnels ainsi que la mise en place de mesures de sécurité, l'accès aux renseignements personnels et les possibilités de correction des données sont en contradiction directe avec les activités du domaine historique.

Secteur des télécommunications et de la câblodistribution

AT&T propose de ne pas exiger que les compagnies de téléphone, pour toutes leurs transactions, soient tenues d'informer les particuliers ou d'obtenir leur consentement pour divulguer des renseignements. Le regroupement de fournisseurs de services de télécommunications va plus loin en précisant que les règles sur la divulgation de renseignements sans consentement doivent suivre les conditions généralement acceptées, dont font état la loi du Québec, la *Loi sur la protection des renseignements personnels* du Canada, la *Loi sur les télécommunications* et les codes sectoriels actuels, comme celui de l'ABC. Il doit être possible d'obtenir des dispenses pour des secteurs en particulier et les propositions en ce sens doivent être déposées auprès du commissaire à la protection de la vie

privée du Canada. Le regroupement de fournisseurs de services de télécommunications propose également que les entreprises de télécommunications soient autorisées à échanger des renseignements sur leurs clients sans obtenir leur consentement dans des situations d'urgence et dans le cas de particuliers débiteurs envers elles, afin d'empêcher ceux-ci d'accumuler des dettes importantes auprès de plusieurs entreprises. Il ajoute que la divulgation de renseignements personnels en vertu d'un pouvoir prévu par la loi ne doit pas nécessiter l'obtention du consentement et que la loi doit tenir compte des cas particuliers des entreprises quand elle définit le droit de retirer un consentement. Le regroupement voit dans l'utilisation et la divulgation de renseignements personnels un outil pour reconquérir des clients, ce qui est un objectif commercial légitime qui ne devrait pas nécessiter d'autre consentement.

Microcell ajoute que la divulgation des renseignements sans consentement doit être autorisée quand il s'agit de protéger la santé et la sécurité, d'appliquer la loi, de se protéger contre des fraudes de la part de clients et de s'assurer que les réseaux interconnectés peuvent fonctionner de façon efficace. Pour l'essentiel, l'ACTS a exprimé le même point de vue que Microcell, ajoutant que la divulgation de renseignements sans consentement doit également être autorisée quand un tiers cherche, de l'avis raisonnable d'un prestataire de services, à recueillir des renseignements personnels à titre de mandataire de l'abonné.

L'ACTC précise que les entreprises ne peuvent être tenues responsables de la collecte, de l'utilisation et de la divulgation de renseignements personnels par un membre du public au sujet de l'utilisation de services et d'installations de communications fournis par les câblodistributeurs alors qu'elles n'ont aucun contrôle direct sur l'information. Dans l'ensemble, Rogers appuie toutes les opinions mentionnées ci-dessus.

Secteur financier

L'ABC énumère plusieurs situations particulières dans lesquelles la divulgation de renseignements sans consentement doit être autorisée. Il s'agit notamment des cas de fraude, de contrefaçon, d'application de la loi, des particuliers mineurs, gravement malades ou frappés d'incapacité mentale et des cas dans lesquels le détenteur des données a établi une relation de mandataire avec le tiers fournissant des services connexes. Il faut alors un contrat pour protéger les renseignements personnels communiqués au tiers. L'OBC propose que la divulgation de renseignements sans consentement se fasse conformément aux dispositions actuelles de la norme de la CSA.

L'ACFC, le Canada Trust, l'ACCAP, Equifax et le CAC sont tous favorables à la divulgation de renseignements sans consentement selon la norme de la CSA. Le Canada Trust estime qu'un code sectoriel constitue le véhicule le plus approprié pour prévoir en détail les modalités pour la divulgation de renseignements sans consentement. Il signale que cette divulgation est exigée dans les cas de relation de mandataire avec un tiers assurant des services connexes. Le CAC précise qu'il faut ajouter à la liste l'« obligation publique » en

faisant référence à la nature des relations qu'il y a entre les assureurs multirisques et les organismes provinciaux d'enregistrements des véhicules qui donnent lieu à l'échange de certains renseignements (par exemple, de données sur les plaintes quand il y va de l'intérêt public) qui ne constituent pas au sens strict une exigence de la loi.

Les commissions canadiennes des valeurs mobilières, les autorités canadiennes en valeurs mobilières et la Bourse de Vancouver affirment que les organismes de réglementation des valeurs mobilières doivent être en mesure de recueillir, d'utiliser et de divulguer des renseignements personnels sans consentement pour mener à bien leur mandat, qui nécessite de faire enquête sur les participants de l'industrie. La Bourse de Vancouver souhaite que la loi prévoie l'exclusion de la collecte de renseignements sur les membres et les entreprises inscrites en précisant que l'on doit refuser l'accès des particuliers à cette information afin de conserver la confiance du public dans l'intégrité des marchés des valeurs mobilières.

CGA Ontario est d'avis que la loi doit prévoir une petite liste de cas particuliers pour la divulgation de renseignements sans consentement, dans différentes circonstances, par exemple, lorsqu'une citation à comparaître ou un mandat de perquisition a été émis, que l'information est déjà publique ou qu'il s'agit d'une situation d'urgence présentant des risques pour la santé et la sécurité ou encore de recherches légitimes où l'information ne sera pas communiquée au public d'une façon qui permette d'identifier la personne visée.

Organisations commerciales (y compris des commerces de détail)

Enlogix est favorable à l'énumération des conditions de divulgation sans consentement de renseignements personnels, comme il est indiqué dans le document de travail d'Industrie Canada. D&B estime que la divulgation sans consentement doit être soumise à des contraintes strictes uniquement lorsque l'information est normalement considérée comme confidentielle et précise que quantité de renseignements sont publics par nature et doivent donc pouvoir être communiqués en toute légitimité au public sans le consentement de la personne visée. D&B ajoute que la divulgation de renseignements est indispensable dans le domaine des transactions de valeurs mobilières et qu'elle doit être permise dans d'autres cas où un tiers est justifié de prendre connaissance des renseignements.

L'ACJ estime qu'il serait ridicule d'autoriser la publication d'articles uniquement lorsque les personnes visées sont satisfaites du contenu. Elle ajoute que l'on doit dispenser clairement de cette obligation dans les cas de publication journalistique étant donné que le recours à la formulation « à moins qu'il ne soit pas approprié » figurant dans la norme de la CSA (*troisième principe*) n'aurait pour effet que de déclencher des poursuites.

Associations du secteur de la technologie de l'information

L'ACFI est d'avis que les renseignements personnels doivent pouvoir être divulgués sans consentement quand cela risque de porter atteinte à la personne ou qu'elle constitue une menace pour d'autres, la divulgation ne se faisant alors qu'auprès des personnes ayant besoin de connaître les renseignements. Elle ajoute que les politiques d'utilisateurs ou les contrats conclus entre les parties qui permettent la divulgation sans consentement constituent un consentement et doivent être reconnus comme tels dans la loi. L'ACI souhaite que la divulgation de renseignements sans consentement soit limitée aux motifs personnels ou impérieux ou aux situations dans lesquelles une organisation est explicitement tenue par la loi de divulguer des renseignements. Elle précise que la divulgation de renseignements en application de la loi ne doit pas être permise dans les cas où un organisme d'application de la loi fait enquête sur ses propres employés. De même, les enquêteurs privés ne doivent pas être autorisés à s'en remettre aux dispositions de la loi pour obtenir la divulgation de renseignements sans consentement. L'ACI est également d'avis que, si la divulgation de renseignements personnels sans consentement doit constituer une infraction, une démarche visant à y accéder sans consentement doit aussi constituer une.

Particuliers (y compris les consultants, les experts et les universitaires)

Les particuliers ont formulé plusieurs suggestions quant aux cas où la divulgation de renseignements sans consentement doit être autorisée. Mentionnons notamment :

- Les alinéas *a* à *m* de l'article 8 (2) de la *Loi sur la protection des renseignements personnels* dans sa forme actuelle constitue un bon point de départ pour l'établissement d'une liste, mais il faut en informer les particuliers lorsque des renseignements les concernant sont divulgués sans qu'ils en aient connaissance ou qu'ils aient donné leur consentement.

- La liste pourrait être plus restreinte que dans le texte actuel de la *Loi sur la protection des renseignements personnels* et la divulgation de renseignements sans consentement, par suite d'une ordonnance d'un tribunal d'un mandat d'un organisme judiciaire, doit être portée à l'attention de la personne visée.

- La divulgation de renseignements à des fins de recherches, de vérification ou d'analyse statistique doit être autorisée avec l'approbation du commissaire à la protection de la vie privée du Canada.

- La divulgation de renseignements sans consentement doit être autorisée par la loi uniquement dans des cas particuliers comme l'écoute électronique.

- Il faut clairement déterminer les circonstances dans lesquelles la divulgation de renseignements est permise et indiquer l'avantage qu'elle présente pour la personne visée ou l'intérêt public.

- La divulgation de renseignements doit être autorisée uniquement lorsqu'elle est absolument nécessaire pour l'exploitation d'une entreprise et chaque divulgation doit alors être consignée.

- Le consentement doit toujours être exigé, sauf dans des cas précis comme lorsque la santé ou la sécurité d'une personne est menacée, notamment dans les cas de risques environnementaux (il a été précisé que, afin de protéger les renseignements personnels, les praticiens de la santé ne doivent pas communiquer tout le dossier médical d'un patient quand ils sont tenus de divulguer des renseignements sur celui-ci aux termes de la loi, par exemple, dans les cas de maladies transmises sexuellement).

- Les médias doivent être autorisés, à des fins d'information, à divulguer des renseignements sans consentement.

- Personne ne doit pouvoir lire le courrier électronique d'autrui sans son consentement, sauf en vertu d'une ordonnance d'un tribunal, et les entreprises privées doivent en informer les employés quand le courrier électronique reçu au travail fait l'objet d'une surveillance.

- Le droit à la protection des renseignements personnels concernant une personne ne doit pas être absolu et les droits de la collectivité doivent l'emporter dans les cas où un comportement de nature répétitive peut nuire à la collectivité.

Faits saillants

Diverses organisations du milieu des affaires et d'autres parties sont d'avis que la divulgation sans consentement de certaines catégories de renseignements doit être possible. D'autres parties, y compris les commissaires ainsi que les groupes de défense des consommateurs, souhaitent que l'on dresse une liste extrêmement limitée et très précise des catégories de renseignements et des situations pouvant donner lieu à la divulgation sans consentement. Certaines parties ont signalé qu'aucune liste de cette nature ne peut être exhaustive. À la lumière des différents points de vue exprimés, la meilleure approche serait peut-être d'inclure une liste détaillée d'exemples de divulgation sans consentement prévus dans la loi, et d'indiquer dans quelles circonstances elle serait normalement permise. On doit également prendre en considération la suggestion formulée par quelques parties, selon laquelle les organisations doivent être tenues de documenter et de justifier la divulgation de renseignements en pareil cas.

3. La nouvelle loi doit-elle reconnaître les codes sectoriels? Dans l'affirmative, doivent-ils avoir force exécutoire? Ou doivent-ils seulement aider à interpréter les principes de la loi pour des secteurs particuliers? Qui doit les élaborer et les approuver?

Un grand nombre de mémoires reconnaissent l'intérêt des codes sectoriels et des codes d'entreprises pour aider les groupes de l'industrie à interpréter la norme de la CSA. Cependant, l'idée de rendre l'application de ces codes sectoriels obligatoire en vertu de la loi, en particulier dans le cas des codes remplaçant la loi, n'a reçu qu'un appui limité.

Quelques mémoires préconisent l'idée de donner force de loi aux codes sectoriels au moyen d'un processus d'approbation gouvernemental. IMS, l'ADC, l'OBC et l'ACMD sont tous en faveur de codes législatifs pour tous les secteurs de l'industrie et d'un système national d'accréditation. Le CAC souhaite que les codes sectoriels aient force exécutoire dans les divers secteurs d'activité et qu'ils soient donc reconnus par la loi à titre d'outils d'interprétation en cas de non-conformité. Donc, quand il s'agit de régler des différends ou de déterminer des sanctions ou des indemnités, un organisme de surveillance doit tenir compte du code auquel l'organisation est soumise et de la façon dont ce code a été appliqué pour déterminer dans quelle mesure la loi a été violée.

Le CPIP propose cependant que, si on donne force de loi aux codes sectoriels, leurs dispositions doivent au moins être équivalentes à celles de loi, sinon les dépasser, s'appliquer à l'ensemble d'un secteur bien défini et pouvoir recevoir l'apport du public.

De toute évidence, l'opinion majoritaire n'est pas favorable à l'adoption de codes sectoriels ayant force exécutoire et remplaçant la loi.

Voici les points de vue exprimés par les diverses parties.

Commissaires

Le commissaire à l'information et à la protection de la vie privée de l'Ontario est le seul en faveur de la reconnaissance des codes sectoriels dans la loi. La Commission d'accès signale que la loi du Québec ne renferme aucune disposition pour la reconnaissance de ces codes.

Le commissaire de l'Ontario précise que les codes sectoriels doivent être reconnus dans la loi et avoir force exécutoire, comme dans le modèle néo-zélandais, tout en signalant que ces codes ne seront guère nécessaires si la loi est bien rédigée. Plusieurs parties visées, dont le ministre responsable, l'organisme de surveillance et un comité de l'industrie, pourraient réviser avant leur approbation les codes sectoriels ayant force exécutoire. Le commissaire met cependant en garde contre la ratification et l'incorporation des codes sectoriels actuels, qui ont été rédigés avant l'adoption d'une loi dans ce domaine.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

La plupart des groupes de défense des consommateurs, notamment la FIPA, le BCOAPO, l'ACC, le CPIP et le Forum sur la vie privée, ainsi que le SCFP sont en faveur du recours aux codes sectoriels uniquement à titre de documents d'interprétation n'ayant pas force exécutoire.

L'ACC de l'Ontario précise que l'utilisation de ces codes pourrait être approuvée par le commissaire à la protection de la vie privée du Canada, mais qu'ils ne doivent pas avoir préséance sur la loi. La BCCLA préconise leur utilisation, sous réserve que des fonds permettent au public intéressé de participer à leur élaboration et à la prise de décisions par consensus. La BCCLA est d'avis que ces codes pourraient bénéficier d'une certaine reconnaissance officielle qui signifierait que le processus d'élaboration a été juste et exhaustif, sans pour autant avoir force de loi.

La FNACQ et OC estiment que ces codes seront efficaces uniquement s'ils ont force exécutoire et ils proposent que l'industrie les rédige, mais que le commissaire à la protection de la vie privée du Canada les vérifie pour s'assurer qu'ils sont bien conformes à la loi.

Le CPIP déclare que, si on autorise des codes ayant force exécutoire, ils doivent être équivalents à la loi, sinon les dépasser, s'appliquer à l'ensemble d'un secteur clairement défini et que le processus d'approbation et d'application des codes doit faire appel à l'apport du public.

Secteur des soins de la santé

L'ADC préconise le principe des codes sectoriels reconnus dans la loi, car elle estime que des menaces particulières à la protection des renseignements personnels imputables aux fusions des sociétés, à toute une gamme de techniques de collecte d'information et à des pratiques de ciblage de marchés sont trop importantes pour être laissées à l'autoréglementation. L'ICIS et IMS souhaitent également que les codes sectoriels soient reconnus par la loi. L'ICIS précise qu'ils doivent être approuvés par des groupes ayant une bonne connaissance du secteur et de la législation sur la protection des renseignements personnels. IMS ajoute que les codes doivent être certifiés et avoir force exécutoires au même titre que la loi.

L'AIIC n'est pas en faveur de la reconnaissance des codes sectoriels en remplacement de la loi.

Administrations publiques (y compris l'Union européenne)

L'Union européenne est d'avis que les codes volontaires n'ayant pas force exécutoire sont utiles mais moins efficaces de façon isolée et plus coûteux à mettre en œuvre et à appliquer.

Associations d'archivistes, d'historiens et de bibliothécaires

Le Comité canadien des affaires législatives et réglementaires préconise l'utilisation des codes sectoriels comme guides n'ayant pas force exécutoire pour adapter les dispositions de la loi. Il exhorte Industrie Canada à encourager l'industrie à déposer ces codes à la Bibliothèque nationale afin de les rendre accessibles au public. La SHC juge que l'utilisation des codes sectoriels pourrait être acceptable s'ils prévoient des politiques de gestion à long terme. L'OLA est en faveur de la reconnaissance de ces codes et de leur caractère exécutoire si tous les intervenants visés en conviennent. L'association précise toutefois que la loi envisagée doit avoir préséance sur tout code sectoriel.

Secteur des télécommunications et de la câblodistribution

Tous les répondants de cette catégorie, à l'exception d'AT&T, sont favorables aux codes sectoriels n'ayant pas force exécutoire préparés uniquement à des fins d'interprétation. AT&T estime que le gouvernement doit définir les exigences pour les codes, que l'industrie rédigerait ensuite et soumettrait à l'examen de l'organisme de surveillance. Les codes pourraient alors avoir force exécutoire dans les secteurs d'activité auxquels ils s'appliquent.

Secteur financier

L'ABC, l'OBC, l'ACCAP, Equifax, les employés Deloitte et le Canada Trust sont tous en faveur de codes sectoriels n'ayant pas force exécutoire et servant à des fins d'interprétation. Le Canada Trust précise que la loi pourrait faire mention du rôle de ces codes. L'ACCAP est en désaccord avec ce dernier point, tandis qu'Equifax précise que des dispositions ayant force exécutoire pourraient être promulguées par la suite si la conformité volontaire donnait des résultats manifestement insuffisants.

Seules deux organisations, l'ACFC et le CAC, prônent la reconnaissance particulière de la valeur d'interprétation des codes sectoriels dans la loi. L'ACFC préfère qu'on reconnaisse la valeur interprétative de codes n'ayant pas force exécutoire. En pareil cas, les divers secteurs de l'industrie devraient élaborer et adopter leur propre code, mais ceux-ci n'auraient pas à être approuvés aux termes de la loi.

Le CAC est aussi d'avis que les codes sectoriels pourraient être préparés par les entreprises d'un secteur d'activité, sans participation du gouvernement, mais qu'ils devraient ensuite être certifiés par des vérificateurs indépendants accrédités et des registraires. Ils

pourraient alors être reconnus par la loi comme ayant force exécutoire pour le secteur d'activité. Le CAC signale que les codes ayant force exécutoire dans l'industrie permettraient de savoir avec davantage de certitude et de mieux prédire comment la surveillance serait faite.

CGA Ontario est en faveur du modèle néo-zélandais, en vertu duquel les codes sectoriels ayant force exécutoire doivent faire appel à l'apport du secteur public et recevoir l'approbation du commissaire fédéral à la protection de la vie privée, qui peut, si les circonstances le justifient, exiger leur révision.

Organisations commerciales (y compris les commerces de détail)

L'ACMD est d'avis que les codes sectoriels doivent être enregistrés auprès d'un organisme national, puis certifiés conformes à la norme de la CSA. Pour sa part, D&B laisse entrendre, en faisant valoir l'expérience limitée de l'industrie dans le domaine des codes volontaires, qu'il est trop tôt pour juger de la façon d'intégrer les codes sectoriels à la loi. Enlogix ne croit pas que les codes doivent avoir force exécutoire et l'ACG ne voit pas la nécessité de codes ou de lignes directrices sectoriels pour le secteur du gaz naturel.

Associations du secteur de la technologie de l'information

Toutes les organisations du secteur sont favorables à des codes sectoriels n'ayant pas force exécutoire, utilisés uniquement à des fins d'interprétation et d'orientation.

Particuliers (y compris les consultants, les experts et les universitaires)

Les opinions exprimées par les particuliers quant à l'intérêt des codes sectoriels vont de l'absence totale d'appui (une perte de temps) à l'approbation de codes n'ayant pas force exécutoire utilisés uniquement à des fins d'interprétation.

Seuls deux particuliers se sont dits d'avis que les codes sectoriels doivent être reconnus officiellement dans une certaine mesure. Un praticien de la santé estime que la loi doit les reconnaître lorsque des groupes comme des comités de déontologie médicale sont tenus de réglementer des organismes professionnels pour protéger le public et qu'ils sont habilités à agréer leurs membres et à imposer des sanctions. Un autre particulier précise que les codes doivent être élaborés par l'industrie et les associations, puis vérifiés par les organismes professionnels reconnus.

Faits saillants

L'appui exprimé à l'égard de la reconnaissance de codes sectoriels ayant force exécutoire est limité. En général, les répondants ont indiqué qu'aucune disposition de la loi ne doit permettre que les codes sectoriels remplacent la loi, ni qu'ils aient une reconnaissance légale, y compris une valeur interprétative. Un mémoire provenant du milieu des affaires, en particulier, a soulevé la question de la valeur interprétative de ces codes (c'est-à-dire que les tribunaux, au moment de déterminer une sanction ou une indemnité, doivent prendre en considération la manière dont l'organisation a interprété la loi en fonction de son code sectoriel). Un mémoire d'un groupe de défense des consommateurs souligne cependant que la nécessité d'empêcher les organisations d'utiliser la « défense impénétrable » selon laquelle elles ont appliqué de bonne foi la norme de la CSA constitue une raison fondamentale pour laquelle la loi doit être plus précise. Étant donné ces opinions incompatibles, il serait peut-être préférable de laisser aux tribunaux le soin de trancher la question de la valeur interprétative, et ce, sans directives dans la loi.

4. Faut-il exclure certains types de renseignements du champ d'application de la loi? Dans l'affirmative, dans quelles circonstances?

Peu de répondants ont formulé des commentaires précis et détaillés en réponse à la question. Le commissaire à la protection de la vie privée du Canada et son homologue de l'Alberta ne souhaitent exclure aucun type de renseignements, tandis que le commissaire de Colombie-Britannique souhaite que la loi resserre son emprise pour s'appliquer aux renseignements biologiques, comme les échantillons de tissu. En ce qui concerne l'exclusion du matériel journalistique, les opinions sont partagées.

Les autres organismes et particuliers ayant formulé des commentaires sur la question ont apporté un appui mitigé à l'exclusion complète du matériel journalistique. Un particulier a proposé qu'on traite de cette question comme le fait la Directive de l'Union européenne qui exclut ces documents du champ d'application de certaines dispositions de la Directive, mais pas de toutes.

Certains sont également d'avis que les renseignements de nature totalement personnelle et non commerciale, comme un répertoire téléphonique personnel ou un album de photos, doivent être exclus du champ d'application de la loi.

Selon une proposition digne de mention, la définition de la notion de « personne » dans la loi doit inclure uniquement les « personnes physiques » pour éviter que les organisations jouissent des droits à la protection des renseignements personnels.

Les réactions sont variées quant à savoir dans quelle mesure des renseignements déjà du domaine public doivent être exclus (si tel est le cas) étant donné qu'il y a des différences notables entre les renseignements du domaine public à vaste diffusion et les renseignements publics qui ne sont en général pas destinés à une vaste distribution ou utilisation. Comme on le verra ci-après, les organisations du milieu des affaires proposent nombre d'exclusions dignes de mention.

Commissaires

En règle générale, les commissaires estiment qu'il ne doit pas y avoir d'exclusions ou que celles-ci doivent être très restreintes. Celui de la Colombie-Britannique est d'avis qu'il faut élargir la gamme des renseignements assujettis à la loi de manière à inclure les renseignements biologiques, comme les échantillons de tissu. Le commissaire de l'Alberta ne préconise l'exclusion d'aucun type de renseignements et celui de l'Ontario ne souhaite pas l'exclusion du matériel journalistique. Quant à elle, la Commission d'accès est favorable à l'exclusion de la collecte, de la conservation, de l'utilisation et de la divulgation de renseignements personnels à des fins journalistiques, comme dans la loi du Québec.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

Seules trois organisations ont répondu directement à cette question, en mettant l'accent sur le matériel journalistique. L'ACC s'oppose à toute exclusion, notamment dans le cas de renseignements recueillis et utilisés à des fins journalistiques. La FNACQ et OC estiment que le matériel journalistique doit être exclu du champ d'application de la loi, comme le prévoit la loi du Québec. Ces organismes sont aussi d'avis que les renseignements utilisés à des fins artistiques doivent être exclus uniquement dans les cas où la personne visée ne peut pas raisonnablement s'attendre à ce que les renseignements personnels la concernant soient protégés et que tous les efforts possibles ont été déployés pour obtenir son consentement. La FIPA est en faveur de l'exclusion pour le matériel journalistique et les dossiers judiciaires et ecclésiastiques ainsi que pour les renseignements compilés et utilisés à des fins strictement personnelles. Elle précise que les renseignements personnels se trouvant dans des archives pourraient bénéficier d'exemptions limitées et soigneusement précisées.

Secteur des soins de la santé

L'ICIS et IMS souhaitent que les données ne permettant pas d'identifier la personne visée soient exclues du champ d'application de la loi.

Administrations publiques (y compris l'Union européenne)

L'Union européenne signale qu'il ne lui a pas semblé opportun d'exclure totalement certains types de données du champ d'application de la loi. À son avis, on peut parvenir à un équilibre mieux adapté en excluant de certains principes différentes activités de traitement des données, par exemple, le journalisme.

Associations d'archivistes, d'historiens et de bibliothécaires

L'AAQ estime que les dossiers et les documents de nature personnelle stockés manuellement sont naturellement protégés et qu'ils doivent donc être exclus du champ d'application de la loi pour autant que l'on ne recueille pas de renseignements portant sur une personne en particulier et que le document ne soit pas informatisé. La SHC réclame avec insistance l'exclusion des données de nature historique, alors que l'OLA souhaite que toutes les données soient exclues quand les liens avec les particuliers ont été supprimés.

Secteur des télécommunications et de la câblodistribution

L'ACTS est d'avis qu'il ne doit y avoir aucune exclusion, tandis que Microcell souhaite l'exclusion du matériel journalistique et laisse entendre qu'il pourrait être

nécessaire d'exclure l'information utilisée pour assurer la sécurité des systèmes de chiffrement à clé publique.

Le regroupement d'entreprises de télécommunications est d'avis que les entreprises de télécommunications ou les prestataires de services œuvrant dans le secteur doivent être dispensés de toute responsabilité quant à l'utilisation que leurs clients font de leurs installations de communications. La loi ne doit pas exiger que ces entreprises assurent le régie ou la protection des renseignements sur lesquels ils n'exercent aucun contrôle direct étant donné la nature des produits et des services qu'elles offrent. Rogers appuie ce point de vue et souhaite par ailleurs que les renseignements ne permettant pas d'identifier la personne visée soient exclus, tout comme ceux qui permettent de remonter uniquement à une adresse de protocole Internet et non pas à un particulier. De même, Rogers exclurait du champ d'application de la loi les données agrégées sur l'utilisation d'Internet qui pourraient servir à des fins de marketing.

Secteur financier

L'ABC estime que l'application de la loi doit être limitée aux renseignements sur les personnes physiques et qu'il faut exclure les renseignements brevetés ou exclusifs afin de ne pas nuire au positionnement concurrentiel des organisations commerciales. L'ACCAP est en faveur des exclusions prévues dans la norme actuelle de la CSA. Le CAC préconise l'exclusion des renseignements sur des particuliers ne permettant pas de les identifier.

Le Western Forum of Credit & Financial Executives signale que les organismes de crédit sont tenus de conserver l'information pendant de longues périodes afin de combattre la mauvaise utilisation du crédit et la fraude dans le domaine. Ils ajoutent que les définitions trop floues relatives aux renseignements personnels présentées dans la norme de la CSA, alliées à des exigences en matière de consentement coûteuses, pourraient se traduire par une forme de censure des données sous prétexte de protection des renseignements personnels, ce qui aurait des effets néfastes pour le secteur du crédit. L'organisme souhaite donc que les renseignements personnels non régis actuellement par les lois provinciales sur l'évaluation du crédit, sur le recouvrement de dettes et sur d'autres domaines connexes soient exclus du champ d'application de la loi sur la protection des renseignements personnels, tout comme les renseignements utilisés pour l'attribution, le prolongement et le recouvrement du crédit. Il ajoute que les renseignements recueillis pour les besoins de contacts d'affaires pourraient être exclus du champ d'application de la loi et que les livres tenus sur une base permanente à des fins commerciales pourraient être considérées comme une propriété privée de l'entreprise qui obtient les données de façon légitime.

Equifax propose également d'exclure les renseignements sur le crédit à la consommation puisqu'ils sont déjà soumis aux lois provinciales. L'entreprise insiste sur le fait que l'exclusion est particulièrement nécessaire s'il n'est pas possible d'assurer l'harmonisation entre les divers secteurs de compétence.

Organisations commerciales (y compris les commerces de détail)

Enlogix propose que toutes les données statistiques ou agrégées soient exclues du champ d'application de la loi s'il n'est pas possible en les manipulant d'établir le lien avec des personnes. D&B est d'avis que les renseignements recueillis sur les entreprises doivent être exclus du champ d'application de la loi et que celle-ci doit s'appliquer uniquement aux personnes physiques.

L'ACJ estime que la collecte de renseignements à des fins journalistiques et pour la constitution d'archives pour les journaux ne doit pas être soumise à la loi pour protéger les valeurs constitutionnelles.

Associations du secteur de la technologie de l'information

L'ACFI est d'avis que le courrier électronique doit être soumis aux mêmes conventions que les autres formes de communications et qu'une partie qui reçoit légitimement des messages électroniques personnels doit être en mesure d'en révéler le contenu ainsi que toute information figurant dans l'en-tête électronique (par exemple, l'adresse de protocole Internet), sans crainte de représailles. À son avis, le commerce électronique ne doit pas être réglementé davantage que le commerce classique et les fournisseurs de services Internet (dont quelques-uns seulement peuvent être assujettis à la loi fédérale sur la protection des renseignements personnels) doivent être en mesure d'utiliser les renseignements figurant dans l'en-tête électronique des abonnés à des fins de marketing, de les louer ou de les vendre à d'autres organisations, comme le font les éditeurs de magazines avec leurs listes d'abonnés.

L'ACI s'inquiète du traitement réservé aux dossiers du domaine public et se demande si une exclusion éventuelle doit s'appliquer à des dossiers en particulier ou à l'ensemble de la base de données. Elle estime aussi que la loi doit préciser si un organisme peut utiliser des dossiers publics à des fins autres que celles pour lesquelles ils ont été constitués à l'origine. Il faut également déterminer si les organisations pourront utiliser des dossiers publics constitués à une fin réglementaire précise pour satisfaire à une autre obligation réglementaire.

Particuliers (y compris les consultants, les experts et les universitaires)

Huit particuliers ont formulé des commentaires qui reflètent des préoccupations tant générales que particulières au sujet de l'exclusion. L'un d'entre eux a déclaré qu'il ne doit y avoir aucune exclusion. Un autre ne souhaite pas que des exclusions dégagent les entreprises de la responsabilité juridique de protéger les renseignements personnels concernant leurs employés et les consommateurs. D'après un troisième, la loi doit s'appliquer de la même façon aux renseignements concernant les employés ou les clients et les contrats de travail ne doivent pas exiger que les employés abandonnent les droits à la protection des

renseignements personnels les concernant. Toutefois, d'opinion contraire, un praticien du domaine de la santé affirme que les organisations qui utilisent des quantités limitées de données doivent être autorisées à s'inscrire et à définir comment elles appliqueraient la norme de la CSA (par exemple, être exclues du champ d'application de la loi), alors que celles qui recueillent et utilisent de grandes quantités de renseignements personnels seraient soumises à une loi précise.

Un autre praticien de la santé estime que des groupes, comme les chercheurs, doivent pouvoir demander à être exemptés de toute assignation à comparaître au sujet de renseignements précis utilisés à des fins de recherche. Il souhaite que des renseignements comme ceux stockés dans le système d'enregistrement de données sur le cancer, dans les dossiers de mortalité et de morbidité de Statistique Canada et dans ceux des admissions et des départs des hôpitaux soient traités de façon différente des renseignements commerciaux du secteur privé.

Un autre particulier affirme que les données rendues anonymes doivent être exclues du champ d'application de la loi et que la liberté de la presse doit s'accompagner de mesures de sécurité. Cette opinion est partagée par un journaliste qui ajoute que la loi doit s'appliquer uniquement aux organisations et non pas aux personnes physiques (y compris les journalistes pigistes). Un autre s'oppose à l'exclusion du matériel journalistique, mais précise que les renseignements personnels concernant tout particulier décédé depuis deux ans, les renseignements recueillis à des fins strictement privées et non commerciales et les renseignements de sources largement connues et facilement accessibles, comme les annuaires téléphoniques, doivent être exclus.

Faits saillants

Les mémoires indiquent que la définition de la notion de « personne » figurant dans la loi doit inclure uniquement les personnes physiques pour éviter que les organisations jouissent des droits à la protection des renseignements personnels dévolus aux particuliers. En outre, les rédacteurs de la loi doivent déterminer s'il est nécessaire d'établir une distinction entre les renseignements du domaine public à vaste diffusion et les renseignements publics qui ne sont pas destinés à une vaste distribution ou utilisation. En ce qui concerne les catégories d'utilisateurs de données, les rédacteurs doivent déterminer s'il convient d'exclure ces utilisateurs de tout le champ d'application de la loi ou de les exclure de dispositions particulières (par exemple, de l'obligation d'obtenir le consentement avant la collecte, l'utilisation ou la divulgation de renseignements).

Pouvoirs

5. Êtes-vous favorable à des obligations initiales telles qu'une inscription destinée à garantir le respect de la loi? Dans l'affirmative, quelle mesure préférez-vous? Qui doit être chargé de surveiller la protection des renseignements personnels?

La majorité des répondants accordent peu d'intérêt à des mécanismes complexes d'enregistrement ou s'y opposent. Contrairement à quelques répondants du milieu des affaires, aucun des commissaires n'appuie le concept. Le dépôt obligatoire des codes et des renseignements sur les contacts auprès du commissaire à la protection de la vie privée du Canada ou auprès d'autres organismes publics ne recueille qu'un appui mitigé. C'est également l'opinion exprimée dans les mémoires présentés par le regroupement de fournisseurs de services de télécommunications, Stentor et l'ACFC.

Cependant, la plupart des groupes de défense des consommateurs et deux particuliers sont favorables à une forme quelconque d'enregistrement initial. La constitution d'un dépôt central des codes et d'un répertoire indiquant les coordonnées des personnes-ressources constitue généralement le principal objectif et la principale raison motivant l'enregistrement. Voici les opinions exprimées sur la question.

Commissaires

Les commissaires s'opposent tous à des obligations initiales telles que l'enregistrement, car ils considèrent ces mécanismes comme étant lourds, coûteux, indûment bureaucratiques et probablement contreproductifs. Comme l'exploitation des systèmes d'enregistrement est souvent confiée aux commissaires responsables des données un peu partout dans le monde, ils sont bien placés pour formuler des commentaires sur l'efficacité de ces modalités.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

Sur les huit groupes de défense des consommateurs qui ont répondu à la question, trois sont contre l'enregistrement initial obligatoire et cinq sont en faveur.

Le Forum sur la vie privée est favorable à l'enregistrement, tout en précisant que le processus ne doit pas être onéreux pour les organisations sans but lucratif ou les petites entreprises et qu'il doit au contraire faciliter l'accès à l'information sur les pratiques et les politiques des organisations. Le CPIP explique que l'enregistrement permettrait d'identifier les utilisateurs de données « à haut risque » ainsi que de détecter et de contrôler les pratiques inappropriées et inacceptables. La tenue du registre devrait incomber à l'organisme de surveillance, qui devrait disposer des ressources nécessaires pour examiner les documents déposés et pour assurer le suivi, allant de simples appels téléphoniques à des vérifications

complètes. Le prélèvement de droits d'enregistrement aiderait à financer les activités d'éducation et de surveillance menées par l'organisme. Toutes les sociétés qui s'occupent de renseignements personnels seraient également tenues de produire un rapport annuel et de rendre publics les renseignements sur la façon dont elles traitent les plaintes.

Le CCC et l'ACC de l'Ontario sont également favorables à l'enregistrement, tout comme l'ACC, qui demande que l'on mette en œuvre des modalités d'enregistrement adaptables à la taille de l'entreprise et à la nature délicate de l'information; les registraires à la protection des renseignements personnels accrédités par le Conseil canadien des normes (CCN) assureraient alors la vérification des tiers. La loi doit préciser les cas où l'auto-enregistrement est autorisé, par exemple, pour les petites entreprises ou pour les renseignements qui ne sont pas de nature délicate.

Secteur des soins de la santé

Seule l'ADC est favorable à l'enregistrement obligatoire, ajoutant que certains secteurs qui traitent de grandes quantités de renseignements personnels pourraient nécessiter une loi particulière. L'ICIS propose que l'enregistrement auprès de l'ACVM ou du commissaire à la protection de la vie privée du Canada soit volontaire.

Associations d'archivistes, d'historiens et de bibliothécaires

Ni le Comité canadien des affaires législatives et réglementaires ni l'OLA ne sont en faveur d'une procédure d'enregistrement initial. Les autres organisations ne font aucun commentaire sur la question.

Secteur des télécommunications et de la câblodistribution

Seuls deux commentaires ont été formulés en faveur d'une modalité quelconque d'enregistrement. Le regroupement de fournisseurs de services de télécommunications est favorable à l'enregistrement des codes sectoriels auprès d'un organisme de surveillance et à la communication du nom de la personne responsable au sein de l'organisation de l'administration des codes. Stentor estime que l'enregistrement peut être utile, mais que les entreprises doivent être libres de l'appliquer où cela leur semble justifié. Stentor propose aussi que les codes adaptés aux divers besoins, accompagnés du nom des personnes-ressources, puissent être accessibles en direct sur un site Web du gouvernement.

Secteur financier

La plupart des répondants qui ont formulé des commentaires sur la question ne sont pas favorables aux obligations ou à un enregistrement initial. Le CAC propose que, en l'absence de plaintes ou de toute preuve manifeste que la protection des renseignements personnels pose un problème, on présume de la conformité à un code. L'OBC précise, à

l'appui de son modèle d'autoréglementation maximale de l'industrie, que les codes doivent faire l'objet de vérifications par des examinateurs accrédités de la protection des renseignements personnels.

L'ACFC propose le dépôt obligatoire des codes auprès du commissaire à la protection de la vie privée du Canada, ce qui semble une solution de remplacement rentable à l'enregistrement. Equifax ne s'oppose pas à un enregistrement volontaire et propose que la modalité devienne obligatoire si le niveau de non-conformité est manifestement élevé.

Seuls les employés de Deloitte sont favorables à l'enregistrement initial et à des vérifications au début. Les résultats des vérifications seraient transmis à un organisme sectoriel, puis à un organisme de surveillance qui exercerait un contrôle. L'organisme sectoriel réviserait périodiquement les politiques de protection des renseignements personnels afin de s'assurer qu'elles demeurent actuelles, compte tenu de l'évolution technologique.

Organisations commerciales (y compris les commerces de détail)

Enlogix est favorable à l'enregistrement initial, avec des codes adaptés dont l'approbation relèverait d'un organisme accrédité par le CCN ou par un organisme gouvernemental en vertu de la loi. L'industrie devrait élaborer ces codes en s'inspirant des conseils de l'ACVM ou du gouvernement. Toute vérification initiale, ou ultérieure, devrait être facultative et menée par des vérificateurs accrédités (tiers) et non par le gouvernement.

L'ACMD est aussi favorable à l'enregistrement des codes. Toutefois, l'ACG s'oppose à l'enregistrement, affirmant que s'il devient obligatoire, les entreprises de services publics doivent en être exemptées pour réduire le fardeau de la réglementation. L'ACG estime aussi que la loi fédérale sur la protection des renseignements personnels constituerait une intrusion dans les domaines du droit des biens et du droit civil qui, en vertu de la constitution, relèvent des provinces.

Associations du secteur de la technologie de l'information

Aucune organisation n'est favorable aux obligations initiales telles que l'inscription. L'ACI préconise une « autodéclaration de conformité » qui serait examinée par l'organisme de surveillance en cas de contestation par un tiers. En échange de cette possibilité d'autoréglementation, les entreprises seraient obligées de très bien tenir leurs dossiers pour faire la preuve de la conformité.

Particuliers (y compris les consultants, les experts et les universitaires)

Sur les sept particuliers qui ont formulé des commentaires sur la question, quatre ne sont pas favorables aux obligations initiales. Parmi les trois autres, l'un souhaite la création

d'un registre de renseignements personnels prenant la forme d'une base de données dans laquelle les entreprises pourront elles-mêmes s'enregistrer quand cela est obligatoire et que le public pourra consulter sur Internet. Un autre propose que les enregistrements volontaires puissent servir de preuves de conformité à la loi, ce qui réduirait les vérifications que le commissaire à la protection de la vie privée du Canada aurait à faire.

Un particulier propose que les entreprises qui envisagent d'utiliser des technologies intrusives, comme l'identification biométrique ou les cartes à mémoire, soient tenues de s'enregistrer ou d'obtenir un permis du gouvernement.

Faits saillants

Ceux qui appuient la mise en place d'un mécanisme d'enregistrement semblent préconiser la création d'un dépôt central de codes et d'un répertoire indiquant les coordonnées des personnes-ressources. Étant donné que les commissaires n'appuient pas ce concept et qu'il est possible, en vertu de la loi, d'obtenir les renseignements en s'adressant directement aux organisations, la mise en place d'un mécanisme d'enregistrement ne semble pas nécessaire.

6. Quels sont les pouvoirs nécessaires pour faire enquête sur des cas éventuels de non-respect et pour régler les différends portant sur les conditions de la conformité avec la loi?

En règle générale, toutes les parties qui ont formulé des commentaires sur la question reconnaissent la nécessité de disposer de pouvoirs d'enquête en cas de plainte. Cependant, les parties n'ont pas toutes fourni une liste détaillée des pouvoirs qui seraient nécessaires pour mener une enquête. Les pouvoirs dont elles font état, le cas échéant, sont le plus souvent en harmonie avec ceux que possèdent actuellement les commissaires. Voici un aperçu des commentaires précis recueillis sur la question.

Commissaires

Le commissaire à la protection de la vie privée du Canada énumère les pouvoirs que lui confère actuellement la *Loi sur la protection des renseignements personnels,* ainsi que des pouvoirs additionnels, y compris celui d'imposer une amende en cas d'entrave manifeste à une enquête, de refuser de faire enquête ou d'abandonner une plainte dans certaines circonstances ainsi que de déposer des plaintes et d'en recevoir directement. Il estime que des pouvoirs seraient également nécessaires pour approuver et contrôler la divulgation de renseignements personnels à des fins de recherche et d'analyses statistiques.

Le commissaire de l'Alberta estime que l'organisme de surveillance doit être habilité à traiter les plaintes et à faire enquête de son propre chef, qu'il doit avoir pleinement droit d'accès aux installations et à l'information, aux dossiers de vérification et aux systèmes de gestion de l'information, être habilité à agir à titre de médiateur dans les différends, à déterminer les délais de réponse, à tenir des audiences, à interroger des témoins, à rendre des ordonnances et à imposer des pénalités en cas d'obstruction manifeste. L'organisme de surveillance doit également pouvoir formuler des commentaires sur les répercussions qu'ont sur la protection des renseignements personnels les nouvelles technologies, les nouveaux services ou les nouveaux programmes et le personnel de l'organisme de surveillance doit être protégé de toute poursuite quand il exerce ses fonctions prévues par la loi.

Le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique estime que les pouvoirs doivent être ceux que définit actuellement la *Loi fédérale sur la protection des renseignements personnels,* avec en plus des pouvoirs réglementaires nécessaires pour régler les différends qui subsistent après l'application des mécanismes de règlement de l'industrie. Le commissaire de l'Ontario établit une liste complète de pouvoirs similaires à ceux énumérés par le commissaire de l'Alberta, y ajoutant le pouvoir de rendre des ordonnances contraignantes assorties de mécanismes de recours complets et efficaces.

La Commission d'accès préconise des pouvoirs comparables à ceux qui figurent dans la loi du Québec.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

La CCIP recommande uniquement l'adoption d'un modèle axé sur les plaintes, selon lequel les consommateurs et les entreprises sont sensibilisés à leurs droits et à leurs obligations. Si les consommateurs ne sont pas satisfaits du traitement de leurs plaintes auprès des entreprises, une enquête indépendante peut alors avoir lieu. Tous les rapports d'enquête de l'organisme de surveillance doivent être mis à la disposition du public par l'organisation faisant l'objet de l'enquête, c'est-à-dire que l'on retiendrait une approche comparable à celle utilisée par le Bureau d'éthique commerciale pour la satisfaction des clients.

Tous les autres groupes de défense des consommateurs sont en faveur de pouvoirs d'enquête plus énergiques. Le FIPA préconise des pouvoirs comparables à ceux que prévoit la loi provinciale sur la protection des renseignements personnels. Le CPIP énumère en détail tous les pouvoirs nécessaires pour faire face à toutes les situations. En plus des pouvoirs déjà mentionnés, il s'agit du pouvoir de rendre publics tous les résultats d'enquêtes et de vérifications, du pouvoir législatif explicite de déléguer certaines fonctions d'enquête ou de vérification à des tiers qualifiés, le pouvoir de promulguer pour l'industrie des règlements régissant les pratiques et les procédures, le pouvoir de percevoir des droits auprès des utilisateurs de données, le pouvoir d'imposer des pénalités en cas de non-conformité et le pouvoir de rendre des ordonnances remédiatrices. Le CPIP ajoute que les particuliers doivent être en mesure d'exiger que l'organisme de surveillance fasse enquête si six adultes formulent des plaintes, comme le prévoit l'article 9 de la *Loi sur la concurrence*.

Secteur des soins de la santé

IMS affirme que la loi doit accorder le pouvoir de demander des vérifications internes ou externes périodiques et l'ADC réclame des pouvoirs d'examen, de vérification et d'imposition de mesures disciplinaires.

Administrations publiques (y compris l'Union européenne)

L'Union européenne propose qu'un organisme de surveillance indépendant soit habilité à vérifier la conformité à la loi, même en l'absence de plaintes.

Instituts

Le Centre de l'Université d'Ottawa est d'avis que les commissaires doivent, en cas de présumée violation à la protection des renseignements personnels, être habilités à recevoir des plaintes, à faire enquête à cet égard et à les régler.

Associations d'archivistes, d'historiens et de bibliothécaires

Le Comité canadien des affaires législatives et réglementaires estime que les pouvoirs doivent être en harmonie avec ceux du commissaire à l'information et à la protection de la vie privée de l'Ontario et comprendre le pouvoir de faire enquête en cas de non-conformité, d'obtenir copie des dossiers, de demander la présentation d'information sous serment, de formuler et de publier des recommandations pour améliorer la conformité, et enfin, de mener des enquêtes de suivi.

L'OLA est d'avis que les organisations doivent d'abord s'occuper elles-mêmes des plaintes reçues, puis faire part de la plainte et de son règlement au commissaire à la protection de la vie privée du Canada . Ce dernier n'aurait alors que des pouvoirs limités de faire enquête dans les cas de violations réelles.

Secteur des télécommunications et de la câblodistribution

Le regroupement de fournisseurs de services de télécommunications propose que les pouvoirs de l'organisme de surveillance soient limités à la réception des plaintes, dont le règlement serait confié aux organismes d'autoréglementation. L'organisme de surveillance ne ferait que vérifier la conformité et mener des enquêtes et des recherches en fonction des besoins. Les parties doivent être tenues par la loi de se réunir et de soumettre à la médiation tout différend.

Stentor est également favorable à un processus axé sur les plaintes, selon lequel les entreprises et les particuliers commencent par tenter de régler les différends, tandis que l'organisme de surveillance a le pouvoir de faire enquête sur les différends, d'agir à titre de médiateur entre les parties et de formuler des recommandations pour améliorer les pratiques utilisées quand les différends ne peuvent être résolus directement entre les parties.

L'ACTS préconise cette approche et ajoute que la loi doit indiquer clairement les principes à respecter dans le cadre des enquêtes sur de présumées violations de la protection des renseignements personnels. L'ACTS précise que toute décision rendue par suite d'une enquête doit être accompagnée des motifs et qu'il faut suivre des procédures juridiques appropriées pour recueillir les renseignements.

L'ACTC et Rogers, qui souhaitent que le CRTC continue d'exercer la surveillance, estiment que les pouvoirs actuellement dévolus à cet organisme pour faire enquête, entendre des témoignages et recevoir des preuves, déterminer les faits et prendre des décisions ayant force exécutoire, sont suffisants pour protéger les renseignements personnels.

Secteur financier

L'ABC et l'OBC sont d'avis que la responsabilité première en matière de surveillance de la protection des renseignements personnels relève des organisations sectorielles. L'OBC précise que, dans les cas où des organismes sectoriels gérés par l'industrie sont en place, l'organisme sectoriel de surveillance doit uniquement formuler des recommandations non contraignantes aux parties à un différend quand celles-ci ne peuvent le résoudre. L'organisme sectoriel de surveillance doit cependant être tenu, par la loi, de rendre compte publiquement des plaintes reçues et de la façon dont elles ont été réglées. L'OBC estime que la menace de rendre compte publiquement devrait constituer un mécanisme suffisamment persuasif pour amener toute entreprise récalcitrante à suivre les recommandations.

Le Canada Trust et Equifax proposent également qu'on s'en remette davantage aux mécanismes mis en place par l'industrie. Le Canada Trust précise que les pouvoirs d'un organisme de surveillance doivent comprendre la prestation de conseils en matière de politique ainsi que l'examen des codes et des procédures des entreprises pour les rares cas où des problèmes demeurent non résolus.

Equifax préconise des pouvoirs d'enquête limités, sans pouvoir d'inspection préventive. L'organisme de surveillance doit être tenu de commencer par renvoyer toutes les plaintes à l'entreprise ou à l'organisme visé, après quoi il aurait le pouvoir de les renvoyer aux organismes provinciaux de surveillance pour les entreprises ou les entités sous réglementation provinciale. Ce n'est qu'après épuisement de ces modalités qu'un particulier aurait le droit de faire appel à un organisme national de surveillance.

Le CAC est favorable à des pouvoirs de surveillance pour mener au besoin des enquêtes et des inspections, mais dans le cadre de limites précises. Il est en effet d'avis que, en l'absence de plainte, l'enquête doit être permise uniquement si on a des motifs raisonnables de croire qu'il y a violation de la loi. Il ajoute que les pouvoirs actuels du commissaire à la protection de la vie privée du Canada, y compris le pouvoir de rendre publics les résultats d'enquêtes, s'ils sont bien adaptés au secteur public, pourraient donner lieu à des ordonnances bien intentionnées, mais erronées, entraînant ainsi pour les assureurs multirisques des conséquences graves et non voulues.

CGA Ontario est favorable à de vastes pouvoirs d'application de la loi, y compris le pouvoir de vérifier les modalités d'utilisation des renseignements et de rendre des ordonnances précises applicables à une entreprise et des ordonnances de nature plus générale concernant des problèmes plus vastes touchant l'ensemble d'un secteur. La loi doit préciser que ces derniers pouvoirs ne peuvent être utilisés que dans des cas exceptionnels et l'industrie doit pouvoir exercer une forme quelconque de recours en révision pour les deux types d'ordonnance.

Les employés de Deloitte souhaitent que l'on habilite par voie législative des organismes sectoriels de surveillance, comme les associations industrielles, à exiger que des tiers procèdent à des vérifications et à des enquêtes, y compris à convoquer et à interroger des témoins, à ordonner la présentation de documents et à prendre des décisions arbitrales. Le plaignant pourrait en appeler d'une décision auprès de l'organisme sectoriel de surveillance, ou d'un organisme de surveillance gouvernemental prévu par la loi, dont les décisions auraient force exécutoire. Les violations du code seraient rendues publiques afin d'inciter les organismes à respecter la loi.

Organisations commerciales (y compris les commerces de détail)

L'ACG envisage uniquement des pouvoirs d'enquête en cas de plainte, selon un modèle de surveillance se rapprochant davantage de celui d'un ombudsman que d'un organisme de réglementation. La loi doit autoriser l'organisme de surveillance à déléguer des pouvoirs et des responsabilités à d'autres secteurs de compétence et à soumettre l'examen des plaintes à des modalités déjà existantes. Il faudrait aussi limiter les enquêtes dans le temps, en imposant des mesures de sécurité pour assurer une protection contre les plaintes frivoles ou répétitives.

Enlogix préconise également des pouvoirs d'enquête et de vérification similaires à ceux d'un ombudsman. L'ACMD réserve son commentaire sur les mesures d'application jusqu'à ce que le détail des modalités soit rendu public.

Associations du secteur de la technologie de l'information

L'ACTP, l'ACFI et l'ACTI estiment que l'on doit recourir à des mécanismes d'application de la loi ou des règlements uniquement en cas de plainte. ACT Canada recommande des pouvoirs plus vastes, laissant entendre que la visite et la vérification de site par l'organisme de surveillance constituent des mécanismes de recours utiles dans certaines situations plutôt que des outils de confrontation. L'ACI précise que l'organisme de surveillance doit être en mesure de contraindre les organisations à fournir des preuves et qu'il faut considérer comme une infraction le fait d'induire en erreur ou de tenter d'induire en erreur l'organisme de surveillance.

Particuliers (y compris les consultants, les experts et les universitaires)

Les particuliers souhaitent le plus souvent des pouvoirs proactifs, comme ceux prévus actuellement par la législation fédérale sur la protection des renseignements personnels, y compris le pouvoir de vérification (deux propositions vont jusqu'à prévoir des pouvoirs équivalant à ceux de Revenu Canada ou des commissaires aux droits de la personne).

On relève deux commentaires supplémentaires formulés par des particuliers, voulant qu'on fasse appel à ces pouvoirs uniquement dans les cas des plaintes les plus graves, en s'inspirant pour l'essentiel des dispositions sur la publicité trompeuse de la *Loi sur la concurrence*, ou quand les organismes sectoriels ont épuisé leurs moyens d'action ou qu'il est probable qu'ils échoueront.

Faits saillants

En général, toutes les parties reconnaissent qu'une entité doit avoir les pouvoirs requis pour faire enquête en cas de plainte. Lorsqu'elles recommandent des pouvoirs détaillés, ils sont généralement en harmonie avec les pouvoirs actuels du commissaire à la protection de la vie privée du Canada.

7. Quels sont les pouvoirs nécessaires pour sanctionner les infractions à la loi et dédommager les personnes qui ont subi un préjudice?

Les groupes de défense des consommateurs et les commissaires sont favorables à de vastes pouvoirs en cas de violation de la loi. La plupart des parties préconisent le pouvoir de rendre publics les plaintes des consommateurs et les cas de non-conformité, sans craindre d'encourir des responsabilités, et y voient l'un des pouvoirs dissuasifs les plus importants.

Les groupes de défense des consommateurs insistent sur le fait que les amendes ne doivent pas devenir un simple coût inhérent à l'exploitation d'une entreprise. Elles doivent être assez élevées pour l'emporter sur les avantages qu'il y a à violer la loi. La plupart des entreprises qui ont répondu à cette question estiment que la détermination des dédommagements pourrait être laissée aux tribunaux, qui imposeraient des amendes proportionnelles aux dommages réellement subis. Voici les commentaires formulés à ce sujet.

Commissaires

Le commissaire à la protection de la vie privée du Canada préconise des modalités de plaintes qui incitent les particuliers à s'adresser d'abord directement aux organisations. Toutefois, dans les cas évidents de non-conformité ou de préjudice envers le particulier, le commissaire à la protection de la vie privée doit pouvoir déterminer les mécanismes de recours appropriés pour le plaignant. Si une organisation n'applique pas les recommandations du commissaire, celui-ci pourra alors rendre publique l'information. En outre, il doit pouvoir renvoyer le cas à la Cour fédérale dans les cas où il serait possible de rendre une ordonnance d'exécution, d'imposer des amendes ou d'indemniser des particuliers.

Le commissaire de l'Alberta est d'avis que le commissaire à la protection de la vie privée du Canada doit posséder les pouvoirs nécessaires pour imposer des pénalités et des sanctions dans les cas d'obstruction intentionnelle, pour déterminer la nature des faits, juger du bien-fondé des plaintes, autoriser les recours et attribuer des dédommagements, limiter la responsabilité dans les cas de recours collectifs et répartir la responsabilité entre ceux qui utilisent et ceux qui traitent les données.

Le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique propose l'imposition de pénalités et de sanctions par voie de poursuites pénales et civiles, alors que celui de l'Ontario préconise le pouvoir d'exiger qu'une organisation modifie ou cesse l'utilisation qu'elle fait de données et d'ordonner la destruction de ces dernières. Le commissaire fédéral doit également pouvoir déposer une ordonnance auprès de la Cour fédérale, ce qui en ferait aux fins de l'application de la loi une ordonnance d'un tribunal. Dans les rares cas où un particulier a réellement subi un préjudice, le commissaire doit être en mesure d'accorder un dédommagement.

La Commission d'accès propose d'imposer des amendes conformément aux dispositions de la loi québécoise.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

Le Forum sur la vie privée estime que l'organisme de surveillance doit être habilité à rendre publics les noms, à ordonner des vérifications, à ordonner la tenue d'enquêtes sur les politiques et les procédures par des tiers, à déterminer des amendes et à accorder des dédommagements.

L'ACC ajoute qu'il faut imposer des amendes lourdes et les majorer en cas de récidive. Le montant doit être établi en fonction du revenu annuel brut du contrevenant et, s'il s'agit d'une violation de la législation sur la protection des renseignements personnels visant à en retirer un avantage personnel, être fonction des gains anticipés. Le CPIP abonde dans le même sens, ajoutant que chaque journée qui passe pendant laquelle l'infraction se poursuit après que le contrevenant en a été avisé doit être considérée comme une nouvelle infraction. Le Centre précise qu'un dédommagement doit être accordé pour la souffrance psychologique, les désagréments et les embarras. Les infractions désignées devraient englober le défaut d'enregistrement, le défaut de rendre compte et le défaut de produire une évaluation des faits sur la protection des renseignements personnels. En vertu de la *Loi sur les contraventions* du Canada, les tribunaux provinciaux doivent considérer qu'il s'agit d'infractions de responsabilité stricte.

Le CPIP ajoute que les citoyens et l'organisme de surveillance doivent pouvoir, par l'intermédiaire du procureur général, intenter des poursuites criminelles ou demander un redressement par voie d'injonction, tant de façon temporaire que définitive. La loi doit également déterminer des limites de temps pour les poursuites de façon à ne pas nuire à l'application de la loi. De plus, les ordonnances de dédommagement doivent permettre aux substituts du procureur de couvrir leurs coûts au moyen des amendes imposées par les tribunaux et de faire en sorte que 50 p. 100 de toute amende soit versée au particulier qui a gagné sa cause. Les particuliers doivent pouvoir aussi intenter des poursuites civiles ainsi qu'un recours collectif et des poursuites indirectes. Il serait possible d'intenter des procédures devant la cour des petites créances et d'obtenir un dédommagement pour la souffrance psychologique, les désagréments et les embarras, suivant une règle selon laquelle l'indemnité minimale est de 500 $, le fardeau de la preuve de diligence raisonnable revenant à l'accusé. Les plaignants qui gagnent leur cause doivent pouvoir obtenir le remboursement de leurs frais juridiques et du coût de l'enquête.

La FIPA appuie, dans l'ensemble, les pouvoirs mentionnés ci-dessus et ajoute que l'organisme de surveillance doit posséder les pouvoirs nécessaires pour approuver ou interdire la collecte indirecte de renseignements personnels. La FNACQ et OC appuient les pouvoirs dont fait état le document de travail d'Industrie Canada, tandis que la BCCLA est

favorable à des modalités de dédommagement conformes à la jurisprudence dans d'autres aspects du droit administratif.

Le SCFP préconise de vastes pouvoirs en matière d'application de la loi, notamment le pouvoir de faire enquête, de délivrer des ordonnances contraignantes, d'imposer des pénalités, de rendre des ordonnances remédiatrices et d'ordonner un dédommagement.

Associations d'archivistes, d'historiens et de bibliothécaires

Le Comité canadien des affaires législatives et réglementaires recommande que la loi renferme des dispositions prévoyant l'imposition d'amendes en cas de violation intentionnelle de la loi, alors que l'OLA préconise des mécanismes ayant force exécutoire pour l'application de la loi, l'imposition de pénalités, comme c'est le cas pour les violations de la législation sur l'environnement.

Secteur des télécommunications et de la câblodistribution

AT&T estime que le fait de ne pas adopter de pratiques équitables dans le domaine des renseignements personnels doit entraîner des conséquences, mais elle signale que la publication d'une liste des entreprises qui ne respectent pas la loi pourrait avoir d'importants effets négatifs sur celles-ci. L'ACTS estime que l'organisme de surveillance doit pouvoir formuler uniquement des recommandations non contraignantes au sujet des plaintes et des problèmes; si aucune mesure n'est prise, la question pourrait alors être renvoyée à la Cour fédérale. L'ACTS estime préférable que les tribunaux aient à trancher les cas de contravention à la loi et à dédommager les particuliers. Le regroupement de fournisseurs de services de télécommunications et TELUS sont aussi d'avis que les pouvoirs d'application de la loi et de dédommagement relèvent des tribunaux.

Stentor est favorable à ce qu'un organisme de surveillance soit habilité à rendre publics les résultats des enquêtes, sous réserve d'un mécanisme d'appel avant la publication, mais elle estime que les parties doivent pouvoir s'adresser à la Cour fédérale pour faire valider le contenu de la loi ou pour vérifier des questions de droit et que les tribunaux provinciaux doivent prendre en charge les questions de dédommagement.

Rogers est favorable au pouvoir d'ordonner des mesures précises, d'imposer un redressement par voie d'injonction et des amendes d'un montant limité en cas de contravention à la loi.

Secteur financier

L'OBC estime que les organismes sectoriels de surveillance doivent être habilités uniquement à formuler des recommandations et à rendre compte publiquement du traitement des plaintes afin d'inciter les entreprises à respecter la loi. Il exprime sa préférence pour un

mécanisme non contraignant et rappelle que les principes de justice naturelle doivent s'appliquer à tout pouvoir de décision ayant force exécutoire accordé à un organisme de surveillance gouvernemental.

L'ACCAP souhaite que les pénalités et les dédommagements soient traités de la même manière que les autres aspects des pratiques commerciales et de la protection des consommateurs, alors que l'ACFC estime que ces éléments relèvent davantage des tribunaux, qui ont une bonne connaissance du droit à la protection des renseignements personnels dans le cadre du code civil. Equifax, entreprise sous réglementation provinciale, signale que la loi de certaines provinces, mais pas de toutes, considère comme un délit l'atteinte à la vie privée et que la plupart des tribunaux provinciaux ont reconnu ce délit dans leur jurisprudence.

Le CAC juge qu'il faut accorder un dédommagement uniquement lorsqu'on a fait la preuve que des dommages ont été subis, et uniquement dans la mesure où la société qui a enfreint la législation sur la protection des renseignements personnels ne peut pas remédier à la situation. Dans de nombreux cas, la solution la plus appropriée serait que l'entreprise en cause corrige les renseignements et transmette les renseignements corrigés aux tiers selon leurs besoins.

CGA Ontario estime qu'il vaut mieux laisser aux tribunaux le soin de déterminer la valeur des dédommagements en espèces, alors que la loi sur la protection des renseignements personnels pourrait prévoir un droit de poursuite civile, comparable à celui qui est défini dans la *Data Protection Act de 1984* du Royaume-Uni. Il s'agit alors de savoir si l'entreprise fera valoir pour sa défense qu'elle a pris des mesures raisonnables en vertu de la loi et quels sont les dédommagements à accorder s'il n'est pas possible de fournir la preuve de dommages.

Les employés de Deloitte ne sont pas favorable à l'imposition de dédommagements, car ils estiment que cela ne ferait que favoriser le dépôt de plaintes. L'imposition d'amendes et la mise en évidence des violations devraient être des éléments dissuasifs suffisants.

Organisations commerciales (y compris les commerces de détail)

L'ACG n'estime pas nécessaire de renforcer la loi actuelle sur la protection des renseignements personnels en ce qui concerne les violations et les dédommagements. Enlogix est favorable à des pouvoirs de médiation et de recommandation, mais non à des pouvoirs coercitifs.

Associations du secteur de la technologie de l'information

ACT Canada est d'avis que le commissaire à la protection de la vie privée du Canada doit être l'organisme de surveillance ultime habilité à la fois à imposer des pénalités

proportionnelles à l'infraction et à attribuer aux victimes un dédommagement en rapport avec les dommages subis. L'ACI est favorable aux ordonnances contraignantes d'un tribunal pour corriger les cas de non-conformité et pour dédommager les particuliers.

Particuliers (y compris les consultants, les experts et les universitaires)

Les particuliers qui ont formulé des commentaires sur la question ont des opinions partagées quant aux pouvoirs dont il faut disposer pour résoudre les cas de contravention et dédommager les particuliers. L'un d'entre eux souhaite que l'on dispose de sanctions limitées, mais estime qu'il faut traiter les dédommagements de façon distincte. Un autre souhaite que le système judiciaire s'occupe des cas de contravention et accorde les dédommagements. Un troisième privilégie un modèle national comparable à celui de Revenu Canada, doté de pouvoirs d'enquête et d'imposition d'amendes à toutes les entreprises, quelle que soit l'administration dont elles relèvent. Un quatrième déclare qu'ils faut se doter des pouvoirs que possèdent actuellement les commissaires. Certains précisent aussi qu'il faut prévoir des pouvoirs de médiation et d'arbitrage pour régler les erreurs sans grande importance commises de bonne foi sans mettre en branle une intervention excessive.

Les quatre particuliers qui ont formulé des commentaires plus précis sur la question des pouvoirs estiment tous qu'il faut pouvoir recourir à des ordonnances ayant force exécutoire, accorder des dédommagements et imposer des amendes. L'un d'entre eux préconise le pouvoir d'ordonner l'interruption des pratiques des entreprises qui contreviennent à la loi et d'imposer des mesures correctrices assorties de vérifications de suivi, et d'obliger les contrevenants à présenter des excuses publiquement et à rendre publics les détails des contraventions. Un particulier propose que les entreprises fautives n'aient pas le droit de vendre de services pendant une période donnée.

Les intervenants qui font état d'amendes sont d'avis que celles-ci doivent être proportionnelles à l'importance, à la nature et à la valeur des dommages éventuels et devraient être assez élevées pour que l'utilisation frauduleuse et délibérée de renseignements personnels ne soit pas simplement un simple coût d'exploitation pour les entreprises. Un autre particulier propose d'imposer à l'entreprise ou à l'employé responsable des amendes pouvant atteindre 100 000 $ à verser à la personne qui a subi le préjudice.

Faits saillants

Les groupes de défense des consommateurs et les commissaires sont favorables à la création de vastes pouvoirs pour sanctionner les infractions. La plupart des parties préconisent le pouvoir de rendre publics les plaintes des consommateurs et les cas de non-conformité, sans crainte de responsabilité, et plusieurs groupes du milieu des affaires et de défense des consommateurs ainsi que des particuliers estiment que ces pouvoirs sont au nombre des plus importants pouvoirs de dissuasion.

8. Faut-il habiliter quelqu'un à mener des recherches indépendantes et une enquête ou une inspection préventives sur les pratiques d'une organisation, et à rédiger des rapports?

La plupart des répondants sont d'avis que les organismes de surveillance doivent être habilités à mener des recherches indépendantes *de nature générale*, car les recherches sur les nouvelles technologies et les questions de protection des renseignements personnels qu'elles posent présentent un intérêt pour toutes les parties.

La tenue d'enquêtes à l'instigation de l'organisme de surveillance recueille un appui partagé. La plupart des mémoires émanant des entreprises s'opposent à ces enquêtes. Parmi les groupes de défense des consommateurs, l'ACC souhaite des pouvoirs d'enquête en cas de soupçons, alors que le CPIP souhaite qu'on utilise la norme de six personnes définie à l'article 9 de la *Loi sur la concurrence* pour déclencher une enquête obligatoire du commissaire à la protection de la vie privée du Canada. Ce dernier est d'avis que le pouvoir de procéder à des vérifications sur des questions précises en cas de plaintes multiples, de faire enquête et d'imposer la médiation laisse entendre qu'il y a des pratiques systématiquement inadéquates dans le domaine de l'information. Les autres commissaires ont exprimé un point de vue similaire. Voici le détail des commentaires sur la question.

Commissaires

Tous les commissaires sont favorables au pouvoir de mener des recherches indépendantes ainsi que des enquêtes et des inspections préventives.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

La FIPA préconise un modèle axé sur les plaintes, tandis que les autres organisations qui ont formulé des commentaires sur la question privilégient en général des pouvoirs proactifs, y compris celui de prendre des mesures en cas de soupçons ou de rumeurs.

Le Forum sur la vie privée signale cependant que seulement 15 p. 100 des répondants à son enquête estiment que la loi doit permettre à tout moment de faire enquête sur une entreprise afin de s'assurer qu'elle respecte bien la loi, sans qu'elle n'ait fait l'objet d'aucune plainte.

Secteur des soins de la santé

L'ADC préconise des pouvoirs d'enquête préventive en précisant que les renseignements personnels ne doivent pas être protégés uniquement en cas de plainte.

Instituts

Le Centre de l'Université d'Ottawa estime que les commissaires doivent être en mesure de déclencher des enquêtes en vérifiant la protection des renseignements personnels et en évaluant les répercussions de la technologie et de mener également des études portant sur la protection des renseignements personnels et les nouvelles technologies.

Associations d'archivistes, d'historiens et de bibliothécaires

L'OLA estime que les commissaires doivent être habilités à mener des recherches et des enquêtes indépendantes uniquement dans le cas de violations réelles de la loi et à procéder à des recherches et à des analyses statistiques uniquement sur des données dont les liens avec des particuliers ont été effacés.

Secteur des télécommunications et de la câblodistribution

Le regroupement de fournisseurs de services de télécommunications n'est pas favorable au pouvoir de mener des inspections et des enquêtes préventives sur les organisations, mais il préconise la possibilité de mener des recherches indépendantes. Rogers et Microcell estiment par ailleurs que le pouvoir de mener des enquêtes préventives est inutile et que l'on doit faire enquête uniquement en cas de plainte. Microcell recommande également que la loi tienne compte du coût des enquêtes et des inspections pour les organisations et permette un recouvrement si une enquête se révèle injustifiée. Les entreprises membres de Stentor ne s'opposent pas à l'exigence de rendre compte des plaintes reçues par les entreprises, à condition qu'il s'agisse d'une procédure habituelle s'inscrivant dans une perspective purement statistique.

Secteur financier

L'OBC, le CAC et Equifax ne sont pas favorables aux enquêtes et aux inspections préventives portant sur les pratiques des organisations en matière de protection des renseignements personnels car la surveillance devrait à leur avis s'exercer uniquement par suite de plaintes. Un organisme de surveillance doit toutefois être en mesure de rendre compte de problèmes systémiques, de surveiller les industries, d'examiner les nouvelles technologies et d'assurer l'éducation du public.

L'ACCAP se contente de dire que le modèle de surveillance doit cadrer avec le traitement des autres aspects des pratiques commerciales et de la protection des consommateurs.

Quant aux employés de Deloitte, ils précisent seulement qu'un organisme de surveillance doit avoir des pouvoirs de contrôle. CGA Ontario est favorable au pouvoir de

vérification et estime que l'organisme de surveillance doit être en mesure d'évaluer les nouvelles technologies.

Organisations commerciales (y compris les commerces de détail)

L'ACG est favorable à ce type de pouvoir uniquement en cas de plainte. Aucun autre commentaire direct n'a été formulé sur la question.

Associations du secteur de la technologie de l'information

ACT Canada préconise la tenue d'enquêtes indépendantes, par exemple, des visites et des vérifications de sites. Les autres organisations ne se sont pas exprimées sur la question.

Particuliers (y compris consultants, experts et universitaires)

Tous les particuliers qui ont formulé des commentaires sur la question préconisent le pouvoir de mener des enquêtes préventives.

Faits saillants

La plupart des répondants sont d'avis que les organismes de surveillance doivent être habilités à mener des recherches indépendantes *de nature générale*, étant donné que les recherches sur les nouvelles technologies et les questions de protection des renseignements personnels qu'elles posent présentent un intérêt pour toutes les parties. La plupart des groupes du milieu des affaires s'opposent à la tenue d'enquêtes préventives, tandis que les commissaires, les groupes de défense des consommateurs et les particuliers sont favorables à la création de vastes pouvoirs pour faire enquête, par exemple, dans le cas où le nombre de plaintes, d'enquêtes et de médiations obligatoires laisse supposer qu'une organisation a des pratiques en matière d'information systématiquement inadéquates.

Répartition des attributions

9. Faut-il créer une autorité centrale qui sera chargée de superviser la mise en œuvre de la nouvelle loi et, dans l'affirmative, quelles doivent en être les attributions? Ces attributions doivent-elles s'ajouter à celles du Commissaire à la protection de la vie privée ou d'un autre organisme?

La vaste majorité des répondants préconisent que le Commissariat à la protection de la vie privée du Canada agisse à titre d'organisme de surveillance.

Quelques mémoires, émanant de groupes précis de l'industrie, ont émis d'autres opinions. L'industrie de la câblodistribution propose de continuer à utiliser son modèle d'autoréglementation en vigueur, sous la surveillance du CRTC. Un répondant du secteur du crédit demande que ce secteur de l'activité économique soit soustrait à la loi. D'autres organismes sous réglementation provinciale font valoir avec insistance qu'ils préfèrent demeurer soumis à la surveillance des organismes sectoriels de réglementation provinciale.

10. Faut-il créer un tribunal ou charger une cour supérieure de rendre des décisions exécutoires suite à des plaintes?

Dans l'ensemble, on observe une légère préférence pour la Cour fédérale par rapport aux autres tribunaux. Le recours à la Cour fédérale recueille encore plus d'appui si des modalités, comme celles proposées par le CPIP *(voir la question n° 7)* sont mises en place pour que les tribunaux provinciaux (par exemple, la cour des petites créances) soient plus facilement accessibles dans les cas de moindre importance. Voici les opinions exprimées sur la question.

Commissaires

Le commissaire à la protection de la vie privée du Canada et la Commission d'accès préconisent le recours aux tribunaux pour obtenir des décisions ayant force exécutoire. La Commission d'accès signale que c'est ce que prévoit la loi québécoise.

Le commissaire de l'Alberta préfère qu'un tribunal rende des décisions finales ayant force exécutoire, en signalant que les tribunaux sont déjà surchargés. Le commissaire de la Colombie-Britannique est d'avis que plusieurs organismes sectoriels comme l'ACMD pourraient juger en première instance dans le cas des différends sur l'utilisation des renseignements personnels, le commissaire à la protection de la vie privée du Canada ayant en dernière instance des pouvoirs exécutoires. Le commissaire doit cependant être en mesure de prendre des recours en révision en cas d'erreur de droit, de partialité, d'absence de compétence et d'autres questions de droit administratif. C'est la Cour fédérale qui doit entendre ces recours.

Le commissaire de l'Ontario est d'avis que le commissaire fédéral doit posséder des pouvoirs exécutoires, mais qu'il devrait y avoir aussi un second niveau d'appel, qu'il ne décrit pas, pour les cas donnant lieu à des versements et à des dédommagements. Le commissaire de l'Ontario estime souhaitable de pouvoir faire appel des décisions qui prévoient des dédommagements.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

La FIPA, le CPIP et la FNACQ et OC préfèrent que l'on ait recours à la Cour fédérale, mais la FNACQ et OC ajoutent qu'une autre solution consisterait à créer un tribunal sur le modèle de celui instauré en vertu de la *Loi canadienne sur les droits de la personne*.

Le CCC, l'ACC de l'Ontario, la BCCLA et le SCFP estiment que les décisions ayant force exécutoire doivent être rendues par un tribunal administratif plutôt que par les tribunaux ordinaires. Le Forum sur la vie privée signale toutefois que la loi doit indiquer

clairement que rien n'empêche les particuliers d'emprunter d'autres voies comme les accusations criminelles et les recours civils.

Secteur des soins de la santé

L'ADC est d'avis que, avec un modèle d'autoréglementation sectoriel, le commissaire à la protection de la vie privée du Canada serait le tribunal de dernier recours.

Gouvernements (y compris l'Union européenne)

L'Union européenne préfère les cours ordinaires et les recours en révision aux tribunaux administratifs.

Associations d'archivistes, d'historiens et de bibliothécaires

Le Comité canadien des affaires législatives et réglementaires estime que le modèle du commissaire à l'information et à la protection de la vie privée de l'Ontario, qui fait office de tribunal administratif habilité à rendre des décisions ayant force exécutoire, est efficace et il n'estime pas nécessaire d'instaurer un autre tribunal. L'OLA préconise que l'on confie le mandat de tribunal administratif au Commissariat à la protection de la vie privée. Ce tribunal aurait pour mandat de régler les plaintes au plus haut niveau et d'imposer des pénalités avec toute la force de la loi.

Secteur des télécommunications et de la câblodistribution

Tous les répondants qui ont formulé des commentaires sur la question privilégient le recours à la Cour fédérale.

Secteur financier

Le modèle de réglementation sectorielle de l'OBC ne laisse pas place à un tribunal administratif ni aux tribunaux ordinaires. L'ACCAP n'a pas exprimé de point de vue clair sur la question, tandis que CGA Ontario et l'ACFC sont en faveur du recours aux tribunaux ordinaires.

Les employés de Deloitte préconisent la création d'un tribunal national en appui aux organismes sectoriels de surveillance. Selon eux, les tribunaux canadiens sont déjà surchargés et les décisions concernant la protection des renseignements personnels doivent être prises rapidement. Le Canada Trust et Equifax sont aussi en faveur de la création d'un tribunal administratif spécial sur la protection des renseignements personnels. Le Canada Trust indique que le tribunal doit être composé de représentants de l'industrie, des

administrations publiques et du public, de la même façon que pour l'Association canadienne des paiements. Equifax est d'avis qu'un tribunal d'appel national doit s'occuper des plaintes contre les secteurs d'activité sous réglementation fédérale ainsi que des appels des décisions rendues par les tribunaux provinciaux.

Organisations commerciales (y compris les commerces de détail)

L'ACG n'appuie pas la création d'un tribunal. Enlogix propose de créer un comité consultatif composé de spécialistes du secteur privé qui conseillerait un nouveau commissaire à l'information et à la protection de la vie privée pour le secteur privé (ne disposant pas de pouvoirs coercitifs).

Associations du secteur de la technologie de l'information

L'ACTP et l'ACTI privilégient le recours à la Cour fédérale. L'ACFI verrait d'un bon œil l'addition d'un tribunal au sein du Commissariat à la protection de la vie privée, dont le fonctionnement se comparerait, par exemple, à celui de la Commission du droit d'auteur, mais elle précise que les parties doivent avoir accès à la Cour d'appel fédérale pour intenter des recours en révision de toute question juridique. L'ACI prône une approche comparable, estimant cependant que les organisations doivent pouvoir faire appel uniquement auprès du commissaire à la protection de la vie privée pour les empêcher d'engager des ressources financières importantes dans un processus d'appel au détriment des particuliers.

Particuliers (y compris les consultants, les experts et les universitaires)

Les opinions exprimées par les particuliers se répartissent à peu près également entre l'audition des appels à la Cour fédérale et la création d'un tribunal administratif ayant le dernier mot en matière de surveillance. L'un des mémoires propose la création d'un tribunal administratif, mais précise que les recours en révision seraient, au besoin, entendus par la Cour fédérale.

Faits saillants

Les avis sont partagés quant au recours aux tribunaux administratifs ou à la Cour fédérale et, en général, les mémoires ne traitent pas à fond des avantages et des désavantages de ces deux approches. La majorité des groupes du milieu des affaires privilégient le recours à la Cour fédérale. Les commissaires et les groupes de défense des consommateurs sont partagés sur la question. Ceux qui privilégient le recours à un tribunal le font généralement pour une question d'accessibilité (les cours sont engorgées); quelques-uns ont proposé que le tribunal agisse à titre d'organisme national qui contribuerait à harmoniser la protection des renseignements personnels dans l'ensemble des provinces et des territoires (d'après certaines parties, le Tribunal des droits de la personne ou le Tribunal de la concurrence pourrait être cet organisme national). Pour ce qui est du recours à la Cour fédérale, certains groupes de

défense des consommateurs indiquent que la loi ne doit pas empêcher les particuliers d'avoir accès à des cours inférieures, comme les cours des petites créances des provinces, pour réclamer des dommages-intérêts. Un groupe de défense des consommateurs propose de mettre en place une approche structurée pour faciliter les poursuites en justice.

11. Quel doit être le rôle des organes de réglementation de l'industrie et des mécanismes sectoriels d'autoréglementation existants? Quelles doivent être les attributions de ces organes s'ils doivent répondre aux attentes des entreprises, des consommateurs et des gouvernements?

En général, toutes les parties sont favorables au concept selon lequel les organisations tentent de régler directement les différends avec les particuliers avant de faire intervenir le commissaire à la protection de la vie privée du Canada.

Certains groupes de l'industrie, en particulier ceux des secteurs des télécommunications et des finances, insistent sur le fait que l'on doit s'en remettre principalement à l'autoréglementation de l'industrie, qui pourrait faire intervenir des organismes d'autoréglementation; le commissaire à la protection de la vie privée interviendrait en dernier recours pour régler les différends dans les cas où les parties n'ont pas réussi à s'entendre ou quand il semble évident qu'elles n'y parviendront pas.

Au sein des secteur des finances et des organisations commerciales, y compris les commerces de détail, quantité d'organisations ont signalé qu'elles relèvent actuellement d'organismes sectoriels de surveillance du niveau provincial et soit qu'elles sont assujetties aux dispositions actuelles sur la protection des renseignements personnels, soit qu'elles s'attendent à ce que ces dispositions soient intégrées aux responsabilités des organismes de surveillance sectoriels.

Malgré la diversité des points de vue exprimés, les répondants semblent en général peu favorables aux rôles comparables à ceux des organismes sectoriels de réglementation du niveau fédéral comme le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) ou le Bureau du surintendant des institutions financières (BSIF). Ils semblent plutôt préconiser fortement que la surveillance relève au bout du compte du commissaire, qui serait secondé au besoin par les organismes sectoriels de réglementation du niveau fédéral, et que l'on recoure aux mécanismes d'autoréglementation de l'industrie quand ils conviennent. Voici un aperçu des opinions exprimées par les parties.

Commissaires

Le commissaire à la protection de la vie privée du Canada estime que son commissariat doit être l'organisme de surveillance ultime, travailler en étroite collaboration avec les organisations-cadres actuelles du milieu des affaires, les associations industrielles et les organismes gouvernementaux visés pour aborder les questions de protection des renseignements personnels par voie de consultations, de conciliation et de négociations et imposer les mesures de coercition et de contrainte absolument minimales. Les organismes sectoriels de réglementation ne doivent selon lui pas jouer un rôle officiel à titre d'organismes de surveillance.

En règle générale, les commissaires provinciaux partagent ce point de vue et incitent les organismes sectoriels à jouer un rôle actif dans le règlement des plaintes et l'élaboration des codes sectoriels.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

Le CCC s'oppose au partage des responsabilités en matière de surveillance de la protection des renseignements personnels avec les organismes de réglementation et les associations industrielles qui existent actuellement. La CPPI privilégie également un organisme central plutôt que des organismes multiples qui traitent les plaintes de groupes ou de secteurs précis de l'industrie. La FIPA, la FNACQ et OC, la BCCLA et l'ACC sont également contre le recours à des organismes sectoriels de réglementation.

L'ACC de l'Ontario et le Forum sur la vie privée préconisent le recours à des organismes de surveillance dirigés par l'industrie, eux-mêmes sous la surveillance du commissaire à la protection de la vie privée. Le CPIP souligne que les organismes sectoriels de réglementation ne doivent servir qu'à diriger les plaignants vers le commissaire à la protection de la vie privée du Canada ou à surveiller un régime de réglementation concurrent. Il précise que le gouvernement doit se protéger contre les entreprises invoquant pour leur défense que leur comportement est réglementé dans le cas des activités précisément autorisées ou sanctionnées par les organismes sectoriels de réglementation.

Secteur des soins de la santé

L'ADC est favorable à l'autoréglemcntation sectorielle sous la surveillance du commissaire à la protection de la vie privée.

Associations d'archivistes, d'historiens et de bibliothécaires

L'OLA, également favorable aux codes sectoriels ayant force exécutoire quand tous les intervenants s'entendent, estime que les organismes sectoriels de surveillance peuvent jouer un rôle de surveillance en appel de première instance quand le particulier et l'organisation visés ne peuvent pas s'entendre.

Secteur des télécommunications et de la câblodistribution

Rogers et l'ACTC estiment que le CRTC doit continuer à jouer son rôle d'organisme de surveillance. Microcell est aussi d'avis que le CRTC peut jouer un rôle utile de façon permanente, puisqu'il a les compétences et le personnel nécessaires pour surveiller les sociétés qu'il réglemente. AT&T et Stentor estiment cependant que les questions de protection des renseignements personnels dans leur secteur ne doivent plus être régies par le CRTC, mais par le commissaire à la protection de la vie privée.

En ce qui concerne les organismes d'autoréglementation de l'industrie, le regroupement de fournisseurs de services de télécommunications préfère continuer à recourir à l'ombudsman actuel des télécommunications, qui agit au nom de plusieurs entreprises. L'ombudsman pourrait renvoyer les plaintes au commissaire à la protection de la vie privée, qui détiendrait le pouvoir final en la matière. L'ACTS indique qu'elle serait prête à recevoir et à entendre les plaintes puis à tenter de les régler au nom des membres de l'industrie, après quoi elle renverrait au commissaire à la protection de la vie privée les plaintes sur lesquelles les parties ne réussissent pas à s'entendre. L'industrie de la câblodistribution signale qu'elle est possède déjà un organisme d'autoréglementation qui fonctionne bien et qu'elle souhaite continuer à y avoir recours.

Secteur financier

De nombreux répondants du secteur financier sont déjà assujettis à des organismes de surveillance propres à leur industrie (par exemple, les organismes de réglementation du secteur des assurances) et qu'ils ont mis en place des mécanismes d'autoréglementation. En conséquence, la vaste majorité des répondants qui se sont exprimés sur la question sont favorables à une utilisation maximale des mécanismes d'autoréglementation de l'industrie et de ses organismes sectoriels de réglementation.

Toutefois, le Canada Trust estime que les associations du milieu des affaires et les ombudsmans de l'industrie n'ont pas l'expérience nécessaire pour surveiller la protection des renseignements personnels et que la loi ne doit pas leur conférer un rôle officiel dans le domaine. CGA Ontario partage cette opinion en précisant que le commissaire à la protection de la vie privée du Canada connaît bien ces problèmes et que la législation actuelle et les mécanismes de protection des renseignements personnels sont au cœur du mandat de son commissariat et non pas une question parmi d'autres qu'il a à traiter.

Organisations commerciales (y compris les commerces de détail)

L'ACG souhaite qu'on utilise au maximum les mécanismes actuels de règlement des plaintes. À son avis, le commissaire à la protection de la vie privée doit pouvoir déléguer ses responsabilités à d'autres secteurs de compétence et faire appel à d'autres mécanismes.

Particuliers (y compris les consultants, les experts et les universitaires)

Neuf particuliers ont traité de la question dans leur mémoire. Deux ne souhaitent pas qu'un rôle soit confié aux organismes sectoriels de surveillance. Un praticien de la santé propose la mise en place d'organismes d'autoréglementation, dont les membres nommés par le public pourraient défendre les intérêts du public en assurant la surveillance des associations professionnelles. Un autre s'oppose vivement à cette opinion, indiquant que seul l'État peut imposer les sanctions qui conviennent. Un particulier souhaite que les organismes sectoriels de surveillance comme le CRTC et le BSIF aient accès à une plus

vaste gamme d'outils d'application de la loi, notamment qu'ils soient habilités à agir de leur propre chef pour régler des plaintes, mais que le commissaire à la protection de la vie privée doit avoir le pouvoir de surveillance ultime. Un autre est favorable au partage des responsabilités dans le domaine de la protection des renseignements personnels, pour autant que l'approche utilisée soit uniforme.

En ce qui concerne les associations industrielles, deux mémoires renferment des commentaires en faveur de leur rôle dans l'éducation du public et de l'industrie et comme « chiens de garde » du secteur industriel, mais ils ne préconisent pas que la loi leur confie un rôle officiel.

Faits saillants

Les répondants estiment généralement que le commissaire à la protection de la vie privée du Canada doit assumer la responsabilité ultime en matière de surveillance. L'attribution de la responsabilité de surveillance ultime aux organismes sectoriels de réglementation sectoriels fédéraux comme le CRTC ou le BSIF ne recueille guère d'appui. Toutefois, certains souhaitent que les organismes d'autoréglementation de l'industrie participent au processus de règlement des plaintes.

12. Qui faut-il charger de l'éducation du public?

Selon l'opinion exprimée le plus souvent par les répondants, l'éducation du public doit relever essentiellement du mandat du commissaire à la protection de la vie privée. Plusieurs répondants ajoutent que celui-ci devrait disposer d'un financement adéquat pour s'acquitter de cette tâche. La Commission d'accès, qui veille à l'éducation du public, fait état d'une proposition récente d'un comité de l'Assemblée nationale du Québec demandant que l'éducation du public soit confiée à la Commission des droits de la personne du Québec. Un répondant propose que Patrimoine canadien et les responsables provinciaux de l'éducation jouent un rôle dans le domaine. Un autre répondant propose que le ministère de la Consommation et des Affaires commerciales joue un rôle dans la diffusion de l'information.

Par ailleurs, les répondants reconnaissent généralement que les responsabilités en matière d'éducation du public doivent être partagées entre les entreprises et l'industrie, les syndicats, les groupes d'intérêt public, les groupes de défense des consommateurs, les associations de l'industrie et d'autres éléments de la société. Un grand nombre d'organisations du secteur privé signalent la transparence des obligations actuelles prévues en vertu de la norme de la CSA en matière de politiques et de pratiques en vigueur dans le domaine de la protection des renseignements personnels. Selon le commissaire à la protection de la vie privée du Canada, la loi doit exiger que les organisations rendent accessibles des renseignements précis sur la façon dont elles gèrent les renseignements personnels et sur les politiques et les pratiques qu'elles mettent en œuvre pour régler les plaintes, sans imposer de coûts ou d'efforts déraisonnables. Microcell propose que le gouvernement s'inspire des recommandations du Comité consultatif sur l'autoroute de l'information pour mettre en place un groupe de travail composé de représentants d'organismes gouvernementaux et de groupes de défense des consommateurs afin de sensibiliser le public à ces questions et de diffuser du matériel éducatif.

Par contraste, l'ACG estime qu'il n'est pas nécessaire d'assurer davantage l'éducation du public, car l'éducation portant sur l'utilisation par le secteur privé de renseignements personnels ne doit pas être plus poussée que celle consacrée à l'utilisation des renseignements personnels par le secteur public.

Le CPIP est favorable à ce que des fonds réservés à l'éducation proviennent de l'enregistrement des utilisateurs de données et de pénalités pécuniaires imposées en cas de non-conformité. Toutefois, comme il est indiqué dans la section portant sur la *question n° 5*, les répondants sont en général peu favorables aux mécanismes d'enregistrement.

Comme la norme de la CSA laisse la nature et l'ampleur de l'éducation du secteur privé à l'entière discrétion de ce dernier, le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique demande que la loi confère un pouvoir partagé entre les commissaires et les industries du secteur privé. Cependant, le commissaire de

l'Ontario estime que cette exigence se révélerait coûteuse et que les entreprises seraient tentées de ne pas en tenir compte.

Plusieurs intervenants ont signalé le rôle des médias. Un mémoire indique que les groupes de défense des consommateurs pourraient jouer un rôle efficace dans l'éducation du public s'ils obtenaient des fonds à cette fin, car ils ont une grande crédibilité auprès du public. Il a également été proposé que les commissaires concluent des partenariats stratégiques avec des entreprises et des associations pour assumer cette responsabilité.

Faits saillants

Selon l'opinion exprimée par la plupart des répondants, l'éducation du public devrait être la principale responsabilité du commissaire à la protection de la vie privée du Canada. Il faudrait préciser dans la loi qu'il s'agit d'une fonction incombant au commissaire et faudrait prévoir les fonds nécessaires pour lui permettre de s'en acquitter. Les organisations doivent avoir l'obligation de faire montre de transparence concernant leurs politiques et pratiques en matière d'utilisation de l'information, comme il est précisé dans la norme de la CSA.

13. La loi doit-elle prévoir l'évaluation des incidences des nouvelles technologies? Dans l'affirmative, quand et par qui?

La plupart des organisations du milieu des affaires s'opposent à ce que la loi exige l'évaluation des incidences des nouvelles technologies sur l'utilisation des renseignements personnels. Elles craignent que l'innovation technologique s'en trouve menacée et qu'un fardeau insupportable accable les petites sociétés disposant de peu de liquidités et que les activités et les emplois soient détournés vers d'autres secteurs de compétence.

La plupart des groupes de défense des consommateurs, mais pas tous, ainsi qu'un ou deux particuliers souhaitent que la loi impose ces obligations. Cependant, parmi les commissaires, seul celui de la Colombie-Britannique préconise ce point de vue.

Les opinions divergent aussi quant à savoir qui devrait procéder aux évaluations. Ainsi, l'ACI estime qu'elles doivent menées ou surveillées par la personne responsable au sein de l'organisation. Les groupes de défense des consommateurs souhaitent pour leur part un mécanisme comportant l'apport et l'approbation du public. Voici un aperçu des opinions exprimées dans les mémoires.

Commissaires

Le commissaire à la protection de la vie privée du Canada estime que son commissariat doit fournir aux organisations les outils nécessaires pour évaluer les incidences des nouvelles technologies sur les renseignements personnels pour toute activité réalisée ou

proposée susceptible d'avoir des conséquences à cet égard. Il n'indique cependant pas clairement si ces évaluations doivent être obligatoires.

Le commissaire de l'Alberta souhaite que les évaluations soient effectuées par l'industrie, puis soumises au commissaire à la protection de la vie privée du Canada de façon volontaire pour obtenir des conseils et des orientations. Il soulève également plusieurs préoccupations pratiques que poserait l'obligation de procéder aux évaluations. Le commissaire précise qu'on aboutirait probablement en pareil cas à un régime dont la gestion serait impossible. Le fait que de nombreux progrès technologiques sont accomplis en dehors Canada et que, en raison de la nature transnationale d'un grand nombre de technologies, il risque de ne pas y avoir de moyen pratique de suspendre leur utilisation jusqu'à ce que l'évaluation soit menée et éventuellement approuvée suscite une préoccupation particulière.

Très favorable à l'évaluation des incidences des nouvelles technologies sur la protection des renseignements personnels, le commissaire de l'Ontario estime que l'organisation qui assure le développement de la nouvelle technologie est la mieux placée pour procéder à l'évaluation, avec l'aide du commissaire. La Commission d'accès ajoute que les entreprises doivent procéder aux évaluations de leur propre chef, car elles sont déjà tenues de se respecter la législation sur la protection des renseignements personnels.

Le commissaire de la Colombie-Britannique soutient toutefois que l'évaluation des incidences doit constituer une condition, exigée par la loi, préalable à la promotion et à l'utilisation des nouvelles technologies de l'information, des nouveaux produits et des nouveaux services qui permettent de recueillir, d'utiliser, de divulguer, de comparer, de relier et de stocker des renseignements personnels. Il faut confier à l'organisation responsable de la technologie, du produit ou du service les évaluations, qui doivent faire état des intérêts opposés conflictuels dans la mesure du possible et préciser la façon de parvenir à un équilibre et, enfin, servir de base pour des consultations menées auprès des commissaires.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

L'ACC de l'Ontario souhaite que le commissaire à la protection de la vie privée du Canada ait pour mandat d'évaluer les incidences qu'ont sur la protection des renseignements personnels les nouvelles technologies dès qu'elles voient le jour. Le Forum sur la vie privée estime que les évaluation doit être obligatoires et respecter une procédure d'évaluation mise au point au moyen de consultations publiques. D'après la FNACQ et OC, les entreprises doivent être tenues par la loi d'informer le commissaire à la vie privée de leurs activités et d'évaluer les incidences avant la mise en marché des services ou, encore mieux, à l'étape de la conception. Chaque évaluation doit être suivie de consultations publiques.

Le CPIP ajoute que les évaluations doivent être obligatoires dans le cas des nouvelles technologies de l'information et que plusieurs organisations doivent y procéder

simultanément afin de permettre de comparer les résultats, soumis au public pour examen et commentaires. Le commissaire à la protection de la vie privée doit être en mesure de demander, au besoin, des évaluations plus approfondies. La loi doit également préciser la signification des expressions « technologies de l'information » et « évaluation des incidences sur la protection des renseignements personnels ».

Toutefois, la FIPA et la BCCLA ne souhaitent pas que les évaluations soient rendues obligatoires. La BCCLA considère qu'elles seraient trop coûteuses et qu'on voit mal les éléments sur lesquels elles porteraient et le rôle exact qu'elles joueraient. Elle estime que l'inclusion d'un principe de justification dans la loi permettrait d'arriver au même résultat, puisque les citoyens pourraient ainsi contester les pratiques inappropriées en matière d'utilisation de l'information. Selon la FIPA, le coût liée au maintien de la norme précédente en matière de protection des renseignements personnels ne doit pas incomber au consommateur lorsque de nouvelles technologies ou de nouveaux services semblent nuire à la protection des renseignements personnels.

Secteur des soins de la santé

L'ADC est d'avis que le gouvernement doit élaborer des principes de base pour l'évaluation des incidences sur la protection des renseignements personnels. L'ICIS estime que la réalisation de telles évaluations devrait lui incomber dans le secteur de la santé.

Instituts

Le Centre de l'Université d'Ottawa estime que le commissaire à la protection de la vie privée doit être habilité à déclencher des enquêtes sur la protection des renseignements personnels, y compris la vérification et l'évaluation des incidences sur la protection des renseignements personnels.

Associations d'archivistes, d'historiens et de bibliothécaires

Le Comité canadien des affaires législatives et réglementaires est d'avis que le commissaire à la protection de la vie privée doit pouvoir demander que les organisations évaluent les incidences sur la protection des renseignements personnels quand elles envisagent de coupler des données. L'OLA estime qu'il n'est pas possible de procéder à des évaluations précises, mais elle propose d'exiger que les nouvelles technologies respectent l'esprit de la loi.

Secteurs des télécommunications et de la câblodistribution

Tous les répondants du secteur s'opposent à ce que l'évaluation des incidences soit rendue obligatoire, indiquant que l'on ne peut présumer que toutes les nouvelles technologies risquent de porter atteinte à la protection des renseignements personnels. En outre, ils

affirment que les évaluations seraient trop coûteuses et trop difficiles à réaliser et qu'elles nuiraient à la position concurrentielle des entreprises canadiennes. L'ACTC est d'avis que l'industrie doit avoir la possibilité de déterminer, sur une base volontaire, si elle doit ou non évaluer les incidences d'une nouvelle technologie et que les réactions du marché sont le meilleur critère quand il s'agit de juger si les technologies visant à améliorer la protection des renseignements personnels donneront ou non de bons résultats.

Secteur financier

Les répondants ont exprimé des opinions partagées. Certains s'opposent à ce que la loi rende obligatoire l'évaluation des incidences. Les employés de Deloitte craignent pour leur part que le fait de « bureaucratiser » le mécanisme en le prévoyant dans la loi nuise à la croissance et à l'innovation technologiques. Selon eux, le marché peut s'autoréglementer dans le domaine. Le CAC se demande comment les résultats des évaluations seraient utilisés. (Les entreprises se verraient-elles interdire d'utiliser ces technologies ou devraient-elles respecter des spécifications?) Le CAC propose que le gouvernement rédige à l'intention des entreprises un ensemble de normes pour leur permettre d'évaluer les incidences des nouvelles technologies, à titre d'aide à la conformité. L'ACCAP ajoute que les entreprises doit évaluer les incidences des nouvelles technologies en développement, sans préciser s'il doit s'agir d'une obligation ou non.

L'ABC estime qu'au lieu de prévoir dans la loi l'évaluation des incidences, il vaudrait mieux informer les consommateurs des risques que présente l'utilisation de nouvelles technologies. Toutefois, selon CGA Ontario, il doit revenir au commissaire d'évaluer les technologies et de vérifier l'utilisation des renseignements au sein des organisations.

Organisations commerciales (y compris les commerces de détail)

L'ACG n'estime pas nécessaire que la loi impose l'évaluation des incidences. Aucun autre commentaire n'a été formulé.

Associations du secteur de la technologie de l'information

L'ACTP, l'ACFI et l'ACTI sont d'avis que le fait de rendre obligatoire l'évaluation des incidences des nouvelles technologies sur la protection des renseignements personnels nuirait grandement à l'innovation et freinerait l'arrivée des nouvelles technologies sur le marché. L'ACTP précise que cette obligation imposerait un fardeau excessif aux petites entreprises disposant de peu de liquidités et que les activités et les emplois qui en découlent se trouveraient détournées vers d'autres secteurs de compétence. ACT Canada n'a pas exprimé de point de vue ferme, mais elle signale avoir collaboré avec le commissaire de l'Ontario dans une évaluation portant sur des cartes à mémoire optiques à la fine pointe de la technologie. En revanche, l'ACI estime qu'il faut évaluer les incidences sur la protection des

renseignements personnels pour tous les nouveaux programmes ou les nouvelles fonctions de gestion et pour les nouvelles technologies, et que celles-ci doivent être réalisées ou surveillées par la personne responsable de la conformité à la loi au sein de l'organisation.

Particuliers (y compris les consultants, les experts et les universitaires)

En règle générale, les particuliers sont favorables à ce que l'évaluation des incidences soit rendue obligatoire dans le cas des nouvelles technologies et de celles qui peuvent porter atteinte à la vie privée. Un particulier demande qu'on y ait recours particulièrement pour les technologies biométriques et les cartes à mémoire, précisant que c'est le commissaire à la protection de la vie privée qui doit en ordonner la réalisation puis décider de permettre ou non l'utilisation de la nouvelle technologie, ou s'en remettre à la décision d'un tribunal administratif spécialisé dans le domaine des renseignements personnels. Deux autres particuliers estiment que le commissaire à la protection de la vie privée doit procéder aux évaluations. Cependant, deux autres estiment que sont des organisations du milieu des affaires qui doivent s'en charger, en suivant les directives du commissaire, et que le résultat doit être soumis à l'examen du commissaire ou rendu publics sur demande. Un particulier est d'avis que le commissaire doit élaborer la norme régissant les évaluations mais il n'a pas précisé qui doit procéder à ces dernières. Un autre réclame la participation d'évaluateurs indépendants et la tenue d'audiences publiques, comme dans le cas de l'évaluation des incidences environnementales.

Faits saillants

Les opinions divergent quant à la nécessité de prévoir dans la loi l'évaluation des incidences qu'ont les nouvelles technologies sur la protection des renseignements personnels. Les organisations du milieu des affaires s'opposent presque à ce que les évaluations soient rendues obligatoires, ce qui pourrait à leur avis nuire à l'innovation technologique, créer des obstacles insurmontables pour les petites entreprises disposant de peu de liquidités et détourner ailleurs les activités et les emplois. Les groupes de défense des consommateurs ont exprimé des opinions partagées concernant les évaluations obligatoires et sur les intervenants qui devraient y procéder. Un seul commissaire souhaite que les évaluations soient prévues par la loi.

Il pourrait être possible de répondre aux intérêts de toutes les parties en protégeant les renseignements personnels, sans avoir une incidence indue sur l'évolution des nouvelles technologies et des nouveaux services, en précisant dans la loi qu'on encourage, plutôt qu'on exige, la réalisation d'évaluations. Les personnes responsables au sein des organisations pourraient procéder aux évaluations, qui pourraient par la suite être examinées dans le cadre de toute enquête ultérieure menée par le commissaire à la protection de la vie privée du Canada.

Coopération

14. Comment les gouvernements fédéral, provinciaux et territoriaux doivent-ils se répartir les responsabilités en ce qui concerne la protection des renseignements personnels dans le secteur privé?

La plupart des organisations du milieu des affaires qui ont répondu à la *question n° 14* estiment que l'harmonisation est importante, voire essentielle, pour la réussite de tout régime de protection des renseignements personnels dans le secteur privé prévu par la loi. L'harmonisation revêt une grande importance en raison des entraves éventuelles au commerce interprovincial, de la nécessité d'un régime efficace et rentable prévu par la loi, de la nécessité de permettre à tous les secteurs de rivaliser à armes égales, des effets nuisibles de l'application de normes différentes pour la protection des renseignements personnels pour le développement et la mise en œuvre du commerce électronique et du désir d'éviter la croissance des refuges de données.

Les commissaires s'entendent sur la nécessité de veiller à l'harmonisation pour assurer l'équité entre toutes les régions du Canada, tout en reconnaissant le partage actuel des pouvoirs.

Lorne Taylor, ministre responsables des Sciences, de la Recherche et des Technologies de l'information pour l'Alberta, est également en faveur de l'harmonisation. Il reconnaît la nécessité d'aller de l'avant avec la loi compte tenu des développements observés en Europe. Le ministre attire toutefois l'attention sur les incidences que pourrait avoir la loi sur les relations commerciales avec les États-Unis et dont il faudrait tenir compte.

En ce qui concerne le calendrier de mise en œuvre d'une législation fédérale sur la protection des renseignements personnels dans le secteur privé, Stentor est d'avis qu'il ne faudrait pas procéder que l'ensemble des provinces et des territoires ne se seront pas clairement engagés à aller également de l'avant. Les autres entreprises de télécommunications sous réglementation fédérale, en particulier TELUS et le regroupement de fournisseurs de services de télécommunications mettent également l'accent sur le déséquilibre concurrentiel que pourrait provoquer une loi uniquement fédérale. Par contre, l'ACTS verrait d'un bon œil une initiative fédérale qui pourrait préciser l'application de la loi pour les autres paliers de pouvoirs publics. Les groupes de défense des consommateurs préconisent fermement eux aussi le leadership du gouvernement fédéral dans le domaine.

Les institutions financières, les compagnies d'assurances et les organismes de réglementation des valeurs mobilières, tout comme les autres organisations fournissant des services financiers, considèrent en général que l'harmonisation constitue un élément essentiel. Précisons toutefois que les institutions financières sous réglementation fédérale n'ont pas indiqué de façon précise si le gouvernement fédéral devrait ou non aller de l'avant le premier. Voici un aperçu des commentaires recueillis sur la question.

Commissaires

La plupart des commissaires préconisent une loi fédérale respectant le partage actuel des pouvoirs constitutionnels, conformément à la *Loi constitutionnelle* de 1867. Le commissaire de l'Alberta verrait d'un bon oeil une loi nationale, entièrement harmonisée afin d'éviter une mosaïque de lois et de règlements incompatibles, peut-être même contradictoires.

Le commissaire de l'Ontario ajoute qu'il faut disposer d'un mécanisme pour résoudre les situations dans lesquelles on ne sait pas avec précision quel ordre de gouvernement est responsable.

Groupes de défense des consommateurs (y compris les mouvements syndicaux)

La FIPA est favorable au partage des pouvoirs entre le commissaire à la protection de la vie privée du Canada et ses homologues provinciaux, conformément au partage actuellement prévu par la Constitution. La BCCLA et l'ACC de l'Ontario estiment que le gouvernement fédéral doit prendre la direction des opérations et être suivi par les provinces. La BCOAPO abonde dans le même sens, ajoutant qu'une loi harmonisée est souhaitable mais non indispensable et qu'une loi fédérale, harmonisée pour l'essentiel avec la loi du Québec doit être adoptée et servir d'exemple pour les autres provinces. Elle ajoute que le gouvernement pourrait faire valoir sa pleine compétence sur la protection des renseignements personnels en raison de sa compétence exclusive sur les télécommunications (puisque des systèmes de télécommunications servent à regrouper, stocker et manipuler de façon électronique les renseignements).

Le CPIP en appelle également aux pouvoirs fédéraux (dans le domaine du commerce, du droit criminel et des compétences générales non attribuées) pour créer un régime national harmonisé, en indiquant que le fait d'être soumis à des réglementations provinciales aboutirait à une véritable mosaïque de normes et de méthodes d'application de la loi. Il précise que la *Loi sur les contraventions* du Canada pourrait, pour des raisons d'efficacité, permettre l'application de la loi par les autorités provinciales, y compris dans les cas de poursuites civiles devant les cours de petites créances.

Secteur des soins de la santé

L'AIIC signale que les soins de la santé relèvent des provinces et souhaite qu'on retienne une approche de coopération permettant d'intégrer la couverture fédérale aux diverses lois provinciales sur la santé.

Administrations publiques (y compris l'Union européenne)

L'Alberta affirme que l'harmonisation est essentielle pour toute future législation sur la protection des renseignements personnels et elle invite fermement le gouvernement fédéral à collaborer avec les provinces avant de rédiger le libellé définitif de la loi. L'apport de la CULC serait aussi très souhaitable avant la présentation de toute loi fédérale proposée.

Associations d'archivistes, d'historiens et de bibliothécaires

Le Comité canadien des affaires législatives et réglementaires préconise une loi nationale ou des lois provinciales harmonisées au sein du secteur privé. L'OLA estime que la loi fédérale doit tenir compte des lois sectorielles et provinciales en vigueur, sur lesquelles elle aurait toutefois préséance.

Secteurs des télécommunications et de la câblodistribution

Tous les répondants font état de la nécessité d'une loi nationale sur la protection des renseignements personnels, harmonisée entre le gouvernement fédéral et les provinces pour éviter de nuire aux secteurs d'activité sous réglementation fédérale et de créer une mosaïque inégale de régimes juridiques. TELUS insiste sur le fait que la législation ne doit pas imposer de fardeau supplémentaire aux secteurs sous réglementation fédérale par rapport aux secteurs comparables de compétence provinciale. Microcell ajoute que la loi ne doit pas nuire aux entreprises qui exercent leurs activités dans plus d'une région du pays.

Rogers et l'ACTS exhortent le gouvernement fédéral à élaborer un système comportant un seul ensemble de lois afin de ne imposer aux entreprises des obligations multiples et éventuellement opposées. Toujours selon l'ACTS, si le gouvernement fédéral prenait le leadership dans le domaine, il pourrait préciser les modalités d'application de la loi pour les autres ordres de gouvernement.

Cependant, Stentor insiste pour que le gouvernement fédéral ne légifère pas tant que les provinces ne se seront pas engagées à aller de l'avant en adoptant des lois harmonisées équivalentes.

Secteur financier

Tous les répondants du secteur insistent sur la nécessité d'assurer l'harmonisation pour en arriver à un norme commune. La CCC ajoute que l'harmonisation dans tous le pays est importante pour les organisations sous réglementation provinciale, comme les coopératives de crédit.

Les opinions divergent cependant sur la façon de parvenir à cette harmonisation. Selon le modèle d'Equifax, une commission nationale au sein du Commissariat à la

protection de la vie privée pourrait exercer la surveillance ultime, à la fois directement sur les sociétés sous réglementation fédérale et par l'intermédiaire d'un mécanisme d'appel dans le cas de tribunaux administratifs provinciaux jugeant des questions de protection de renseignements personnels. En vertu du modèle de l'OBC, qui fait appel dans une large mesure à l'autoréglementation de l'industrie, le rôle du commissaire à la protection de la vie privée se limiterait à renvoyer les plaintes vers les organisations sectorielles et à surveiller les résultats, ce qui limiterait la nécessité de l'harmonisation des lois fédérales et provinciales.

L'ACIFA et le Canada Trust estiment que le gouvernement fédéral doit remplacer, regrouper ou reporter les lois actuelles qui créent des conflits et des doubles emplois, y compris les lois qui régissent les établissements des secteurs financiers et des assurances sous réglementation fédérale et provinciale.

Organisations commerciales (y compris les commerces de détail)

La Chambre du commerce du district de Sudbury affirme que la loi doit être souple, cohérente et applicable dans tous les secteurs de compétence. L'ACG considère que l'harmonisation est indispensable et précise que la loi fédérale doit s'en tenir uniquement aux principes et prévoir la délégation des pouvoirs fédéraux aux provinces afin d'éviter le double emploi des procédures.

L'ACMD propose un modèle comparable à celui de la *Loi canadienne sur la santé*, en vertu duquel le gouvernement fédéral établit des normes de base minimales en laissant à la discrétion des provinces l'application précise et détaillée.

Associations du secteur de la technologie de l'information

Toutes les associations du secteur accordent une grande importance à l'harmonisation. ACT Canada recommande que la portée de la loi aille de pair avec la répartition actuelle des pouvoirs déterminée par la *Loi constitutionnelle de 1867* et par les lois connexes ultérieures.

Particuliers (y compris les consultants, les experts et les universitaires)

Tous les particuliers qui ont formulé des commentaires sur la question déclarent que l'harmonisation est importante pour assurer le caractère universel du droit à la protection des renseignements personnels au Canada et pour garantir la reconnaissance internationale (par exemple, pour respecter les exigences de la Directive de l'Union européenne). Dans l'ensemble, les répondants sont d'avis que chaque administration doit légiférer dans son propre domaine de compétence.

Cependant, un particulier propose la création d'un Conseil canadien de la protection des renseignements personnels pour surveiller la mise en œuvre de la protection des renseignements personnels dans tout le pays, mais aurait uniquement le pouvoir d'enquêter et de formuler des commentaires.

Faits saillants

La plupart des parties estiment que l'harmonisation est importante, voire essentielle, pour la réussite de tout régime de protection des renseignements personnels dans le secteur privé prévu par la loi et pour le marché. Pourtant, elles donnent peu d'instructions précises sur la façon d'assurer l'harmonisation. Les opinions sont partagées quant à savoir si le gouvernement fédéral devrait agir unilatéralement et adopter une loi sans attendre que les provinces fassent de même.

15. Quelles instances, en plus de celles dont il est question dans le présent document, peuvent contribuer à l'harmonisation de la protection des renseignements personnels à tous les paliers de gouvernement au Canada?

De nombreux répondants mentionnent la CULC, ce qui montre bien que le projet actuel de l'organisme, qui consiste à rédiger une loi-type sur la protection des renseignements personnels, est bien connu et que les répondants sont favorables au rôle que pourrait jouer ce genre de modèle. Il a également été mentionné que d'autres instances permettraient de réaliser des progrès sur le plan de l'harmonisation, par exemple, les réunions régulières des commissaires, les Conférences des premiers ministres, les conférences annuelles des ministres de la Justice et des procureurs généraux, la réunion des ministres responsables de l'autoroute de l'information, les agents principaux de l'information des provinces, le Comité interprovincial du commerce intérieur et du Conseil consultatif de l'infostructure sur la santé (affecté au ministre de la Santé).

Certains mémoires demandent que les associations du milieu d'affaires, les syndicats, les groupes de défense des consommateurs, le secteur de la santé, les archivistes, les organismes sectoriels de réglementation et les autres principales parties intéressées participent activement aux instances supplémentaires qui seront mises en place pour examiner la législation sur la protection des renseignements personnels, tant au niveau fédéral que provincial.

Faits saillants

De nombreux répondants se réjouissent du travail accompli par la CULC, qui rédige actuellement un avant-projet de loi-type sur la protection des renseignements personnels. Toutefois, on doit aussi faire appel à d'autres instances pour faire progresser l'harmonisation de la protection des renseignements personnels dans tous les secteurs de compétence. Les instances doivent faire intervenir le plus possible les parties intéressées.

Conclusions générales

Les résumés et les analyses présentés dans le présent document ne peuvent pas du tout rendre justice aux commentaires réfléchis et structurés qu'ont formulés toutes les parties sur la question de la législation de la protection des renseignements personnels dans le secteur privé. Un grand nombre de commentaires de nature générale sur la protection des renseignements personnels dans notre société technologique n'ont pu trouver leur place ici, même si beaucoup d'entre eux étaient dignes de mention.

Le processus de consultation a donné lieu à 90 mémoires, dont de nombreux documents complets et détaillés traduisant, en général, l'intérêt que portent tous les Canadiens à la protection des renseignements personnels et à l'atteinte d'un équilibre entre les divers intérêts.

La convergence manifeste des opinions exprimées et l'ampleur des compromis semblent indiquer qu'il serait possible, en déployant des efforts supplémentaires, de parvenir à équilibrer les intérêts et à ainsi tenir compte des intérêts légitimes de toutes les parties. La norme de la CSA constitue de toute évidence un bon point de départ pour l'adoption d'une loi, même s'il est nécessaire de déployer des efforts supplémentaires pour atteindre le degré de précision souhaité, examiner les obligations additionnelles proposées par certaines parties et chercher les meilleures façons de tenir compte des besoins des journalistes, des agences d'évaluation de crédit, des organismes de réglementation des valeurs mobilières, des chercheurs en médecine, des archivistes et des autres parties touchées par la législation sur la protection des renseignements personnels.

En outre, les répondants sont nettement favorables à ce que le commissaire à la protection de la vie privée du Canada exerce un rôle de surveillance et ils conviennent de la nécessité de certains pouvoirs d'enquête préventive et de l'éducation du public. Les répondants sont également favorables aux mécanismes de règlement des plaintes qui commencent au niveau des organisations du milieu d'affaires et ils souhaitent que l'on encourage fortement ces organisations à élaborer en la matière des codes de pratique sectoriels qui serviront de guide.

On constate également que pratiquement toutes les parties prônent l'élaboration d'un cadre national de lois harmonisées sur la protection des renseignements personnels dans le secteur privé, qui s'appliquerait dans tous les secteurs de compétence afin de doter tous les Canadiens de mesures équivalentes de protection des renseignements personnels et d'assurer que toutes les entreprises puissent rivaliser à armes égales dans le domaine. La mise en place de ce cadre devrait constituer l'objectif le plus important pour faire progresser la législation sur la protection des renseignements personnels.

Annexe 1

LISTE des mémoires reçus en réponse au document de travail

1) Mémoires des organisations

Association canadienne des compagnies d'assurances de personnes inc. (ACCAP)	1089
Association canadienne de l'informatique (ACI)	1084
Association canadienne de la technologie des cartes (ACT Canada)	1062
Association canadienne de technologie de l'information (ACTI)	1043
Association des infirmières et infirmiers du Canada (AIIC)	1046
Association canadienne des journaux (ACJ)	1047
Association canadienne de technologie de pointe (ACTP)	1030
Association canadienne des télécommunications sans fil (ACTS)	1070
Association canadienne de télévision par câble (ACTC)	1083
Association canadienne du gaz (ACG)	1034
Association canadienne du marketing direct (ACMD)	1016
Association dentaire canadienne (ADC)	1086
Association des archivistes du Québec (AAQ)	1077
Association des compagnies financières canadiennes (ACFC)	1028
Association des consommateurs du Canada, section ontarienne (ACC de l'Ontario)	1002

Association canadienne des institutions financières en assurance (ACIFA)	1037
Association des banquiers canadiens (ABC)	1092
Association des consommateurs du Canada (ACC)	1060
Association canadienne des fournisseurs Internet (ACFI)	1085
Autorités canadiennes en valeurs mobilières (ACVM)	1079
B.C. Civil Liberties Association (BCCLA)	1063
B.C. Freedom of Information and Privacy Association (FIPA)	1061
BC Public Interest Advocacy Centre (B.C. Old Age Pensioners' Association, Consumers' Association of Canada B.C. Branch, Council of Senior Citizens' Organizations, Federated Anti-poverty Groups of B.C., Senior Citizens' Association of B.C., West End Seniors' Network, B.C. Coalition for Information Access, End Legislated Poverty et Tenants' Rights Coalition (BCOAPO)	1057
Bourse de Vancouver	1045
Cabinet de comptables agréés Bennett Gold, Robert Y. Gold	1026
Canada Trust	1059
Centrale des caisses de crédit du Canada (CCCC)	1080
Centre pour la promotion de l'intérêt public (CPIP)	1039
Centre de recherche et d'enseignement sur les droits de la personne, Université d'Ottawa	1065
Certified General Accountants Association of Ontario (CGA Ontario)	1066
Chambre de commerce métropolitaine de Halifax	1017
Chambre du commerce du district de Sudbury	1091
Coalition canadienne de l'information publique (CCIP)	1021
Comité canadien des affaires législatives et réglementaires d'ARMA International	1055

Commissaire à l'information et à la protection de la vie privée (Ontario), Ann Cavoukian 1027

Commissaire à la protection de la vie privée du Canada, Bruce Phillips 1076

Commissaire à l'information et à la protection de la vie privée (Columbie-Britannique), David H. Flaherty 1018

Commissaire à l'information et à la protection de la vie privée (Alberta), Robert C. Clark 1078

Commission d'accès à l'information du Québec 1095

Conseil d'assurances du Canada (CAC) 1048

Conseil canadien de la consommation (CCC) 1093

Deloitte et Touche (Yezdi Pavri, Robert Parker, Adel Melek, Brenda Eprile, Ian Tod, Karen Nemani et Nina Vivera) 1074

Dickson, Gary, C.R., député de Calgary-Buffalo, assemblée législative de l'Alberta 1067

Dun & Bradstreet Canada 1031

Enlogix Inc 1049

Entreprise AT&T Canada Inc. 1041

Equifax Canada Inc. 1023

Faneuil ISG Inc. 1075

Fondation des normes de télévision par câble (FNTC) 1044

Forum sur la vie privée (Réseau Éducation-Médias, Centre pour la promotion de l'intérêt public, Coalition canadienne de l'information publique, Association des consommateurs du Canada, Télécommunautés Canada, Fédération nationale des associations de consommateurs du Québec et Bibliothèque publique d'Ottawa) 1073

Fraser Institute 1015

Gendarmerie royale du Canada (GRC) 1033

IMS Canada (IMS) 1032

Institut d'histoire de l'Amérique française (IHAF) 1069

Institut canadien d'information sur la santé (ICIS) 1071

Microcell Télécommunications Inc. 1052

Ministre responsable des sciences, de la recherche et de la technologie de l'information (Alberta), Lorne Taylor 1036

Ombudsman bancaire canadien (OBC), Michael Lauber 1025

Ontario Library Association (OLA) 1058

Option consommateurs (OC) **et Fédération nationale des associations de consommateurs du Québec** (FNACQ) 1038

Regroupement de fournisseurs de services de télécommunications : ACC TelEnterprises Inc., AT&T Canada services interurbains, Call Net Enterprises Inc., fONOROLA Inc. et Westel Telecommunications Ltd. 1040

Rogers Communications Inc. 1042

Société historique du Canada (SHC) 1020

Stentor Politiques publiques Télécom Inc. (Bell Canada, B.C. TEL, Island Tel, MTS, MT&T, N.B. Tel, NewTel Communications, NorthwesTel, QuébecTel, SaskTel, B.C. TEL Mobility, Bell Mobilité, Island Tel Mobility, MTS Mobility, MT&T Mobility, N.B. TEL Mobility, NewTel Mobility, QuébecTel Mobilité, SaskTel Mobility, NorthwesTel Mobility) 1054

Syndicat canadien de la fonction publique (SCFP) 1088

TELUS Corporation 1051

Union européenne, M. John Mogg, directeur général, DG XV, Marché intérieur et services financiers 1081

Western Forum of Credit and Financial Executives 1022

2)Mémoires des particuliers

Bennett, Chris 1056

Bobier, Paul 1006

Brown, Glen R.	1013
Campbell, Terry, indie IDEAS	1035
Clement, Andrew, professeur agrégé à l'Université de Toronto	1064 (1068)
Fallis, Richard	1005
Fletcher, Tim, police régionale de Hamilton-Wentworth	1029
Harris, Don, HR Systems, New York Times Company et président du comité de l'IHRIM sur l'utilisation et la protection de l'information	1053
Huband, Ken, Information Management Services	1014
Kuethe, Christopher	1009
Laninga, Ken	1007
Laughlan, Colin	1050
Litwyn, Jay	1008
Maurel, Richard-Philippe	1010
McNaughton, D.M.	1019
Meek, Chet	1004
Newcombe, Howard B.	1003
Siebert, Andreas	1011
Soskolne, Colin	1012
Speers, Richard D.	1072
Williams, Colin J.	1024